Arja Kotkansalo • Leena Parkkila • Jaana Tarvainen

B

Riskianalyysimenetelmien tarkastelu

Kirjallisuusselvitys

LAPIN AMKIN JULKAISUJA
Sarja B. Tutkimusraportit ja kokoomateokset 23/2017

Riskianalyysimenetelmien tarkastelu - kirjallisuusselvitys

Arja Kotkansalo • Leena Parkkila • Jaana Tarvainen

Riskianalyysimenetelmien tarkastelu

Kirjallisuusselvitys

Sarja B. Tutkimusraportit ja kokoomateokset 23/2017

Lapin ammattikorkeakoulu
Rovaniemi 2017

ISBN 978-952-316-199-3 (nid.)
ISSN 2489-2629 (painettu)
ISBN 978-952-316-200-6 (pdf)
ISSN 2489-2637 (verkkojulkaisu)

Lapin ammattikorkeakoulun julkaisuja
Sarja B. Tutkimusraportit ja
kokoomateokset 23/2017

Rahoittajat:
Lapin Liitto, Euroopan unioni -
Euroopan aluekehitysrahasto,
Vipuvoimaa EU:lta 2014-2020

Kirjoittajat: Arja Kotkansalo,
Leena Parkkila, Jaana Tarvainen

Kansikuva: Arja Kotkansalo
Taitto: Lapin AMK, viestintäyksikkö

Lapin ammattikorkeakoulu
Jokiväylä 11 C
96300 Rovaniemi

Puh. 020 798 6000
www.lapinamk.fi/julkaisut

Lapin korkeakoulukonserni LUC
on yliopiston ja ammattikorkea-
koulun strateginen yhteenliittymä.
Konserniin kuuluvat Lapin yliopisto
ja Lapin ammattikorkeakoulu.
www.luc.fi

Sisällys

Tiivistelmä

Parhaillaan käynnissä olevan TPA – Tuotannon poikkeama-analyysi – hankkeen (1.10.2015 – 30.9.2018) lähtökohtana ja tavoitteena on kehittää TPA menetelmää kaikille teollisuuden aloille sopivaksi analyysimenetelmäksi, jolla voidaan tunnistaa sekä turvallisuuden, ympäristön että talouden kannalta kriittisten poikkeamien esiintyminen niiden tuotantoprosesseissa. Hankkeen aikana, TPA menetelmässä, pyritään yhdistämään tunnetuimpien analyysimenetelmien parhaat ja kuvaavimmat osatekijät yhdeksi helppokäyttöiseksi kokonaisuudeksi.

Tämä kirjallisuusselvitys kuuluu TPA – Tuotannon poikkeama analyysi – hankkeen (1.10.2015 – 30.9.2018) työpakettiin 2, jossa tarkoituksena on selvittää yleisimpien riskianalyysimenetelmien (VVKA, HAZOP, RCA ja riskianalyysi) parhaat puolet ja karsia päällekkäiset vaiheet uuden työkalun tapauskohtaiseen luomiseen.

Kirjallisuusselvityksessä tarkastellaan eri riskianalyysimenetelmien vahvuuksia ja etuja sekä rajoituksia ja puutteita. Lisäksi tarkasteltiin eri menetelmien päällekkäisyyksiä. Tuloksena saatiin kirjallisuusselvitys yleisimmistä riskianalyysimenetelmistä ja niiden eri yhdistelmistä. Selvityksessä on käytetty apuna mm. eri kirjallisuus-, Internet-, raportti- ja artikkelilähteitä.

Kirjallisuusselvityksen mukaan mikään riskianalyysitekniikka yksinään ei ole riittävä hallitsemaan riskejä vaan riskinarviointiprosessi voidaan parhaiten saavuttaa järjestelmällisellä lähestymistavalla käyttäen erilaisia analyysien yhdistelmiä.

Yhdistämällä eri analyysejä pyritään hyödyntämään menetelmien parhaat puolet ja löytämään niistä käyttökelpoisimmat osa-alueet TPA menetelmän luomista varten. Tämä kirjallisuusselvitys toimii pohjana työpaketille 3 TPA-menetelmän kehittämiseksi, jotta menetelmää voidaan testata case-kohteissa ja lopulta tuottaa geneerinen TPA-menetelmä teollisuuden tarpeisiin.

Asiasanat
riskianalyysi, analyysimenetelmä, tuotannon poikkeama-analyysi, turvallisuus, ympäristö, talous, poikkeama

1 Johdanto ja taustaa

Teollisessa toiminnassa käytetään useita eri menetelmiä, jotta havaittaisiin ja pystyttäisiin ennakoimaan tuotanto-omaisuuden häiriö- ja ongelmatilanteita. Menetelmiä on kehitetty vuosia ja osa niistä on saavuttanut lähes standardimaisen aseman. Menetelmien kirjo aiheuttaa aika ajoin myös ongelmia johtuen mm. siitä, että niiden sisällöt ovat, tarkoituksesta huolimatta, samankaltaisia ja päällekkäisiä. Standardin SFS-EN 31010 mukaan eri riskinarvioinnissa käytettäviä työkaluja on listattu reilut 30 kappaletta, jotka näkyvät taulukossa 1.

Taulukko 1. Riskinarvioinnissa käytettävien työkalujen ja tekniikoiden kirjo. (SFS-EN 31010, 2013)

Työkalut ja tekniikat	Riskinarviointiprosessi					Katso Liite
	Riskin tunnistaminen	Riskianalyysi			Riskin merkityksen arviointi	
		Seuraus	Todennäköisyys	Riskitaso		
Aivoriihi	SA[1)]	NA[2)]	NA	NA	NA	B 01
Ohjatut tai osittain ohjatut haastattelut	SA	NA	NA	NA	NA	B 02
Delfoi	SA	NA	NA	NA	NA	B 03
Tarkistusluettelot	SA	NA	NA	NA	NA	B 04
Alustava vaara-analyysi	SA	NA	NA	NA	NA	B 05
Poikkeamatarkastelu (HAZOP)	SA	SA	A[3)]	A	A	B 06
Vaara-analyysi ja kriittiset seurantapisteet (HACCP)	SA	SA	NA	NA	SA	B 07
Ympäristöriskien arviointi	SA	SA	SA	SA	SA	B 08
Rakenne « Mitä jos? » (SWIFT)	SA	SA	SA	SA	SA	B 09
Skenaarioanalyysi	SA	SA	A	A	A	B 10
Liiketoiminta-analyysi	A	SA	A	A	A	B 11
Juurisyiden analyysi	NA	SA	SA	SA	SA	B 12
Vika- ja vaikutusanalyysi	SA	SA	SA	SA	SA	B 13
Vikapuuanalyysi	A	NA	SA	A	A	B 14
Tapahtumapuuanalyysi	A	SA	A	A	NA	B 15
Syy- ja seurausanalyysi	A	SA	SA	A	A	B 16
Syy-ja vaikutusanalyysi	SA	SA	NA	NA	NA	B 17
Kerrossuojausanalyysi (LOPA)	A	SA	A	A	NA	B 18
Päätöspuu	NA	SA	SA	A	A	B 19
Ihmisen luotettavuuden analyysi	SA	SA	SA	SA	A	B 20
Rusettianalyysi	NA	A	SA	SA	A	B 21
Toimintavarmuuskeskeinen kunnossapito	SA	SA	SA	SA	SA	B 22
Piilopiirien analyysi	A	NA	NA	NA	NA	B 23
Markov-analyysi	A	SA	NA	NA	NA	B 24
Monte Carlo simulointi	NA	NA	NA	NA	SA	B 25
Bayestilastot ja Bayesverkot	NA	SA	NA	NA	SA	B 26
FN käyrät (uhriluvut)	A	SA	SA	A	SA	B 27
Riski-indeksit	A	SA	SA	A	SA	B 28
Seuraus/todennäköisyys matriisi	SA	SA	SA	SA	A	B 29
Kustannus/hyöty analyysi	A	SA	A	A	A	B 30
Monikriteerianalyysi (MCDA)	A	SA	A	SA	A	B 31

[1)] Erittäin soveltuva (SA).
[2)] Ei soveltuva (NA).
[3)] Soveltuva (A).

Toteutettaessa menetelmien mukaisia analyysejä tehdään usein päällekkäistä työtä ja siten heitetään aikaa hukkaan. Taulukossa 2 on esitetty arviota, kuinka kauan erilaisten menetelmien läpiviemiseen kuluu aikaa. Taulukossa 3 on esitetty, keiden prosessihenkilöiden osallistumista vaaditaan menetelmien läpiviemiseksi. (US_EPA, 2008)

Taulukko 2. Ajallinen arvio eri menetelmien läpiviemiseksi. (US_EPA, 2008)

Various Steps	Checklist	What-if	What-if/ Checklist	HAZOP	FMEA	FTA
Simple/Small System						
# Staff	1-2	2-3	2-3	3-4	1-2	2-3
Preparation	2-4 h	4-8 h	6-12 h	8-12 h	2-6 h	1-3 d
Modeling						3-6 d
Evaluation	4-8 h	1-3 d	6-12 h	1-3 d	1-3 d	2-4 d
Documentation	4-8 h	1-2 d	4-8 h	2-6 d	1-3 d	3-5 d
Large/Complex Process						
# Staff	1-2	3-5	3-5h	5-7	2-4	2-5
Preparation (hours)	1-3 d	1-3 d	1-3 d	2-4 d	1-3 d	4-6 d
Modeling						2-3 w
Evaluation	3-5 d	4-7 d	4-7 d	1-3 w	1-3 w	1-4 w
Documentation	2-4 d	4-7 d	1-3 w	2-6 w	2-4 w	3-5 w

Note: h = hours; d = days (8 hours); w = weeks (40 hours)

Taulukko 3. Menetelmien läpiviemiseen tarvittava henkilöstö. (US_EPA, 2008)

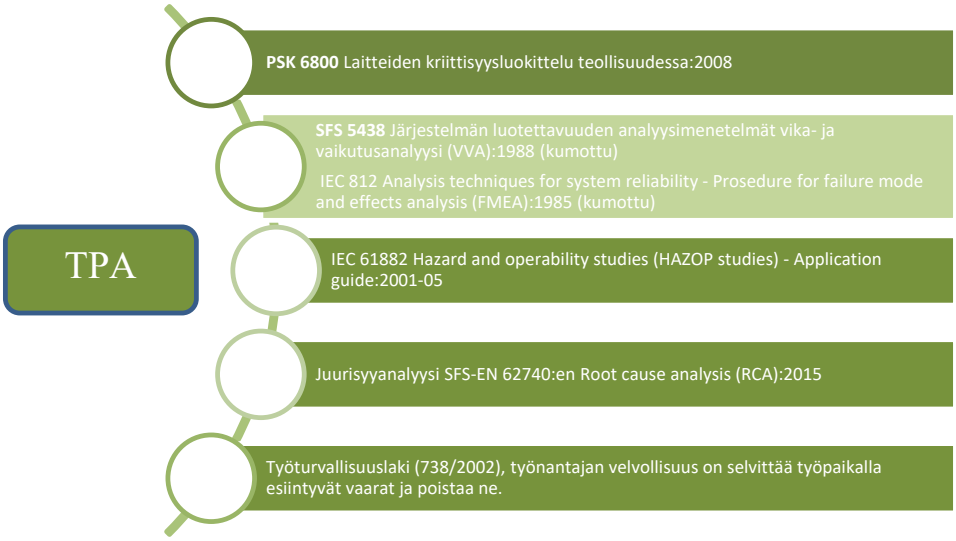
Particular Phases in Process Design and Operation	Checklist	What-if	What-if/ Checklist	HAZOP	FMEA	FTA
R&D		✓				
Design	✓	✓	✓			
Pilot Plant Operation	✓	✓	✓	✓	✓	✓
Detailed Engineering	✓	✓	✓	✓	✓	✓
Construction/Startup	✓	✓	✓			
Routine Operation	✓	✓	✓	✓	✓	✓
Modification	✓	✓	✓	✓	✓	✓
Incident Investigation		✓		✓	✓	✓
Decommissioning	✓	✓	✓			

Joissain tapauksissa myös saatujen tulosten painotus ei ole johdonmukainen ja loogi-nen. Väitettä tukevat mm. vika-, vaikutus- ja kriittisyysanalyysia käsittelevässä SFS-EN 60812:en:2006 standardissa listatut puutteet. Lisäksi Kemi-Tornion ammattikor-keakoulussa tehdyn tapaustutkimuksen laskennan tuloksena saatiin, että tehtäessä PSK 6800 mukaista tarkastelua ympäristö- ja turvallisuuskriittiset laitteet peittyvät kokonaiskriittisyyden arvioinnissa. Myös laskennan avulla kohdentuvat toimenpiteet eivät aina ole laajasti hyödynnettävissä, yhden keskittyessä tuotannon käytettävyy-teen, toisen turvallisuuteen jne. Aiemmin tehdyssä SULKA-hankkeessa Oulun yli-opiston kanssa tuli esille, että tarkastelua, jossa laajemmin otettaisiin huomioon sekä tuotannon kokonaistehokkuus että turvallisuus- ja ympäristöriskit, ei nykyisellään ole olemassa (Rauhala, ym., 2014). Tämän kirjallisuusselvityksen aikana tuli esille, että em. ei ehkä pidä enää paikkaansa. Jos tarkasteluun otetaan nyt löydetyt muualla maailmassa käytössä olevat kombinaatiot, niitä on siis jo käytössä. Näistä yhdistelmä-menetelmistä kerrotaan lisää kappaleessa 5.

Tuotantoprosesseja tarkastellaan jo nyt erilaisten analyysien avulla. Vika-vaikutus-kriittisyysanalyysi (VVKA) tarkastelee tuotantoprosessin materiaali- ja laiterikkojen taloudellista sekä turvallisuus ja ympäristö vaikutusta. Poikkeamatarkastelu (HA-ZOP) tutkii prosessisuureiden muuttumisen vaikutusta turvallisuuteen. Myös erilai-silla riskianalyysimenetelmillä kartoitetaan prosessin käyttöön liittyviä turvallisuus-riskejä. Lapin AMKin toteuttamissa tutkimushankkeissa on havaittu, että näistä

analyysimenetelmistä mikään ei yksinään riitä tuotantoprosessin kokonaisvaltaiseen turvallisuus-, ympäristö- ja taloudellisten riskien hallintaan. Toisaalta nämä eri analyysimenetelmät sisältävät myös samoja elementtejä, jolloin tietyt asiat joudutaan käsittelemään useaan kertaan eri menetelmiä käytettäessä.

Meneillään olevan Tuotannon poikkeama-analyysi (myöhemmin TPA) hankkeen yhtenä tavoitteena pyritään kokoamaan yleisimpien menetelmien; vika-, vaikutus-kriittisyysanalyysin (VVKA), poikkeamatarkastelun (HAZOP) ja riskianalyysin parhaat puolet, poistamaan niiden epäkohdat sekä karsimaan päällekkäisiä vaiheita. TPA-hankkeessa kehitettyä menetelmää täydentää juurisyyanalyysi (RCA; Root Cause Analysis), jolla pyritään tarkentamaan poikkeamatarkastelua. Kuvassa 1 on esitettynä standardit ja lait, jotka olivat lähtötietoina TPA-menetelmän kehittämiseen.

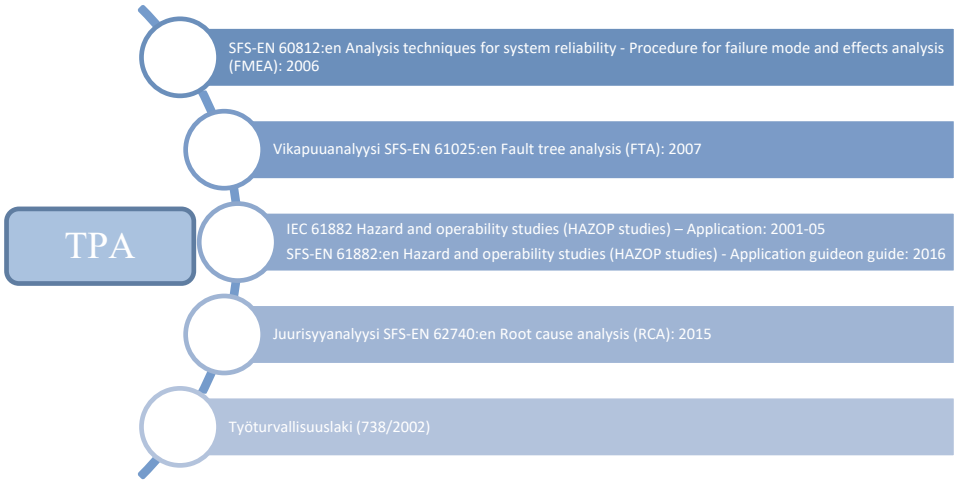


Kuva 1. Kehitysvaiheessa ensimmäisen TPA-menetelmäversioon liittyvät standardit ja lait. Kumottu SFS 5438 on esitetty vaaleanvihreällä.

Kansainvälisestä IEC 812:1985 Analysis techniques for system reliability - Prosedure for failure mode and effects analysis (FMEA) standardista on tehty suomennos SFS 5438:1988 ”järjestelmän luotettavuuden analyysimenetelmät vika- ja vaikutusanalyysi (VVA)” standardi, mutta se on vanhentunut ja kumottu ja siksi kuvassa 1 vaaleanvihreänä. (SFS 5438, 1988)

Myös tämä vanha IEC 812:1985 standardi on kuitenkin vanhentunut ja kumottu. Edellä mainitusta standardista päivitetty englanninkielinen versio on vuodelta 2006; SFS-EN 60812:en Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA). Kyseinen standardi on yleisesti käytössä kansainvälisesti ja se sisältää kriittisyystarkastelun sekä ohjeistaa riskiprioriteetti laskelman (Risk Priority Number, RPN) käytön. Kuvaan 2 on listattu TPA menetelmään liittyvät tämänhetkiset uusimmat standardit.

Tämän kirjallisuusselvityksen yhtenä tarkoituksena on selvittää yllä kuvattujen standardien kuvaukset, käyttö ja soveltuvuus. Julkaisussa tuodaan esille myös muita menetelmiä, jotka ovat sidoksissa riskianalyysin tekemisessä. Harva menetelmä yksistään riittää ja usein tarvitaan toisia riskianalyysimenetelmiä täydentämään arviointia. Tästä syystä on syytä tarkastella eri menetelmien kombinaatioita, joita on käyty läpi julkaisun lopussa.



Kuva 2. Kehitteillä olevassa TPA-menetelmässä kansainvälisesti käytössä olevat riskianalyysimenetelmät (standardit)

2 Riskien hallinta ja arviointi

Riski on läsnä kaikessa ihmisen toiminnassa. Se voi liittyä terveyteen, turvallisuuteen, talouteen tai vaikuttaa ympäristöön. Riskienhallinnan tavoite on valvoa, ehkäistä tai pienentää menetyksiä, jotka aiheutuvat hengen menetyksestä, sairaudesta tai vammasta, omaisuusvahingoista ja seurausvahingoista sekä ympäristövaikutuksista. (SFS-IEC 60300-3-9, 2000)

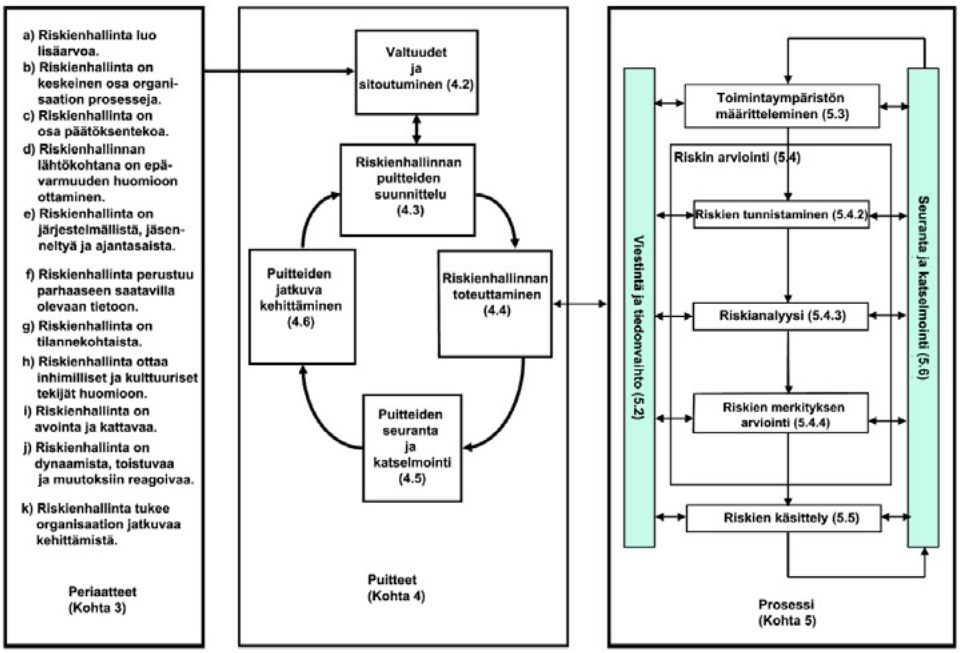
Riskienhallinnan teoreettinen kenttä on laajahko ja se sisältää loogisten ja systemaattisten menetelmien soveltamisen. Riskienhallintaprosessi on riskienhallinnan toteuttamista käytännössä (SFS-EN 31010, 2013). Hallintaa ja prosessia kuvaa hyvin standardi nimeltään riskienhallinta, periaatteet ja ohjeet SFS-ISO 31000:2011. Riskienhallinnan periaatteiden, puitteiden ja prosessien väliset suhteet on esitetty kuvassa 3. Luotettavuusjohtaminen, teknisten järjestelmien riskianalyysi standardi SFS-IEC 60300-3-9 pureutuu syvemmälle riskianalyysi aiheeseen. Riskien hallinta, riskien arviointimenetelmät standardissa SFS-EN 31010:2013 annetaan ohjeita riskien arvioinnin perusperiaatteista ja erityyppisistä riskienarviointitekniikoista.

Viimeksi mainittu standardi esittää hyväksi havaittuja käytäntöjä vastaavat keinot riskin arviointitekniikan valitsemiseksi ja käyttämiseksi. Se on yleisluontoinen eli sitä voidaan käyttää monille teollisuusaloille ja järjestelmätyypeillä ja sitä voivat käyttää kaikki julkiset ja yksityiset yritykset, yhteisöyritykset, järjestöt, ryhmät tai yksittäiset henkilöt toimialasta tai sektorista riippumatta. SFS-EN 31010 standardin mukaan riskien arviointi on:

> *”Riskin arviointi on se osa riskienhallintaa, joka tarjoaa järjestelmällisen menetelmän, jolla tunnistetaan mahdolliset vaikutukset tavoitteisiin. Se myös analysoi riskin sen seurauksien ja niiden todennäköisyyden kannalta ennen kuin päätetään vaaditaanko lisätoimenpiteitä.*

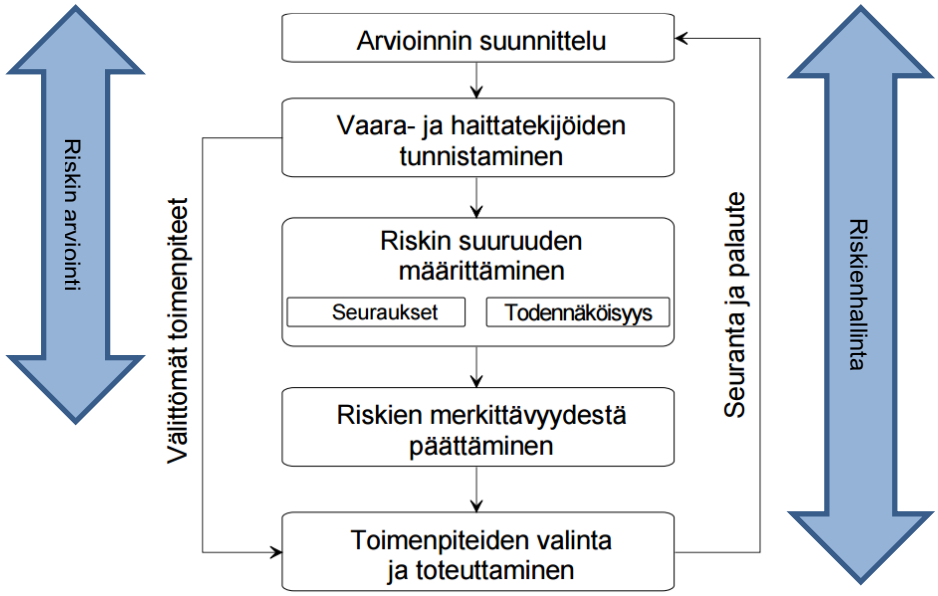
Riskin arviointi yrittää vastata seuraaviin olennaisiin kysymyksiin:

- *Mitä voi tapahtua ja miksi (tunnistamalla riskin)?*
- *Mitkä ovat seuraukset?*
- *Mikä on todennäköisyys niiden tapahtumiselle tulevaisuudessa?*
- *Onko mitään tekijöitä, jotka lieventävät riskin seurauksia tai jotka pienentävät riskin todennäköisyyttä?" (SFS-EN 31010, 2013)*



Kuva 3. Riskienhallinnan periaatteiden, puitteiden ja prosessien väliset suhteet (SFS-ISO 31000, 2011)

Tarkempi riskienhallinnan prosessi on esitetty kuvassa 4. Prosessi etenee vaiheittain ja se aloitetaan kohteen lähtötietojen keräämisellä ja arvioinnin suunnittelulla. Tämän jälkeen tunnistetaan vaara- ja haittatekijät ja arvioidaan jokaisen vaaratekijän aiheuttaman riskin suuruus, sen seuraukset ja todennäköisyys. Tämän jälkeen arvioidaan jokaisen riskin hyväksyttävyys. Suuria riskejä ei hyväksytä ja niiden poistamiseksi tai pienentämiseksi sovitaan toimenpiteet, nimetään vastuuhenkilö ja aikataulu. Sovittujen toimenpiteiden toteutumista seurataan ja toimenpiteiden jälkeen kyseisen kohteen riskiarviointi tehdään uudelleen. (Työturvallisuuskeskus, 2015)



Kuva 4. Riskien arviointi ja hallinnointi (Työturvallisuuskeskus, 2015, s. 7)

Työturvallisuuslain 10§ mukaan työnantajalla on velvollisuus työn vaarojen selvittämiseen ja arviointiin (Työturvallisuuslaki (738/2002)). Työn vaarojen tunnistamiseen ja riskien arviointiin on olemassa useita erilaisia apulomakkeita (Työturvallisuuskeskus, 2016_a), mutta kokonaisuutena analyysimenetelmää ei ole standardisoitu tietyllä lomakkeella tehtäväksi.

2.1 RISKIENARVIOINTI

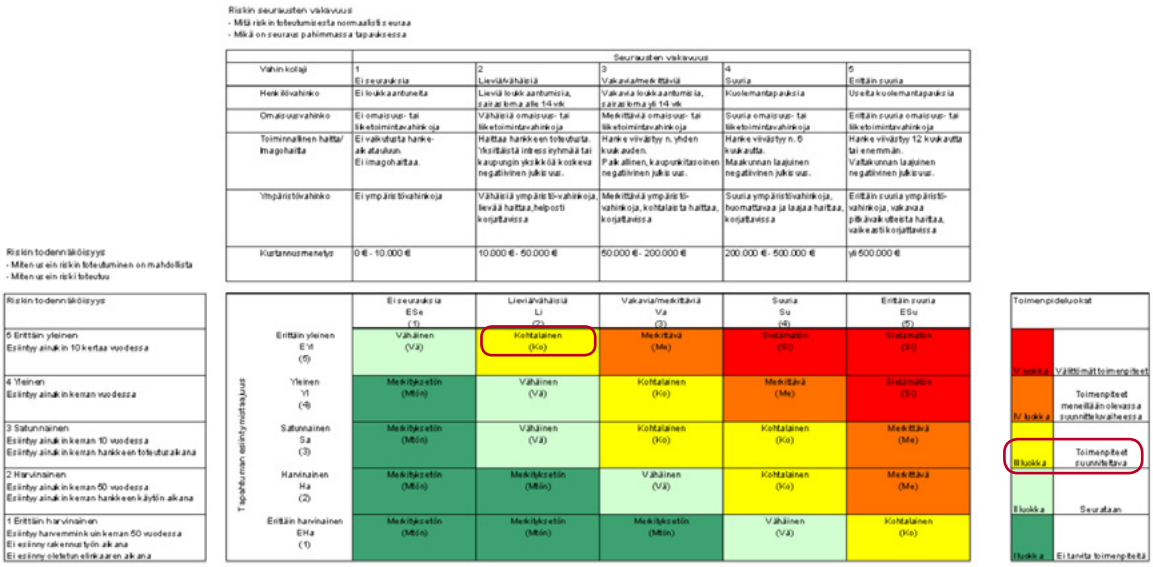
Riskin arviointi on riskin tunnistamisen, riskianalyysin ja riskin merkityksen arvioinnin kokonaisprosessi (katso kuva 3). Tapa, jolla tätä prosessia sovelletaan, ei riipu ainoastaan riskienhallinnan toimintaympäristöstä, vaan myös niistä menetelmistä ja tekniikoista, joita käytetään riskin arvioinnin suorittamiseen. Riskin arviointi voi vaatia monitieteellistä lähestymistapaa, koska riskeillä saattaa olla monitahoisia syitä ja seurauksia. (SFS-EN 31010, 2013) Liitteeseen 1 on koottu yhteen SFS-EN 31010 standardissa mainittuja työkaluja ja/tai menetelmiä, jotka soveltuvat riskienarviointiin sekä riskianalyysin tekemiseen; erittäin soveltuva (++), soveltuva (+) ja ei soveltuva (-). Myös standardi SFS-IEC 60300-3-9 antaa ohjeita riskianalyysin tekniikoiden valitsemiseksi ja toteuttamiseksi. Joitain useimmin käytettyjä riskianalyysimenetelmiä on taulukkoon korostettu teksteillä. Luettelo ei kuitenkaan ole missään suhteessa täydellinen. Toisinaan saattaa olla tarpeen käyttää useampaa kuin yhtä analyysimenetelmää.

Ryhmä, joka riskienarvioinnissa käytettyjä työkaluja ja menetelmiä käyttää, on tavallisesti monitieteellinen ja se sisältää suunnittelu- ja käyttöhenkilöitä. Näillä henkilöillä tulee olla sopiva tekninen asiantuntemus arvioida poikkeamien vaikutusta aiotussa tai nykyisessä suunnitelmassa. On suositeltavaa, että ryhmässä on jäseniä, jotka eivät suoraan ole vastuussa tarkasteltavan järjestelmän, prosessin tai menetelmän suunnittelusta. (SFS-EN 31010, 2013)

2.1.1 Riskin tunnistaminen

Riskien tunnistamisen tarkoituksena on ehkäistä ne riskit, jotka toteutuessaan vaikeuttavat tai estävät organisaation keskeisten tehtävien suorittamista. Riskien tunnistamisessa voidaan hyödyntää erilaisia riskien koontitaulukoita, joihin luettelomaisesti kerätään mahdolliset riskit. Riskit voidaan arvioida määrällisesti, esimerkiksi kuvan 5 riskimatriisin avulla todennäköisyyden ja seurausten vakavuuden mukaan. Lisäksi toimenpiteet priorisoidaan riskien suuruuden mukaan. (Rantanen, 2014)

Esimerkiksi arvioitavan riskin seurausten vakavuus on lievä/vähäinen (2) ja todennäköisyys, että se esiintyy ainakin 10 kertaa vuodessa, eli se on erittäin yleinen (5). Kuvan 5 mukaan riskin todennäköisyys ja seurausten vakavuus ovat kohtalainen ja sille on suunniteltava toimenpiteet. Näistä saadaan aineistoa kriisinhallintasuunnitelmaan tai toimenpideohjelmaan.



Kuva 5. Eräs esimerkki riskimatriisista (Rantanen, 2014)

Kuvassa 6 on esitetty laadullisesta/sanallisesta riskimatriisista esimerkki.

Tapahtumataajuus	Arvioitu taajuus (vuodessa)	Seurausten vakavuus			
		Pieni	Vakava	Suuronnettomuus	Katastrofaalinen
Hyvin todennäköinen	>1	Keskinkertainen riski	Korkea riski	Korkea riski	Korkea riski
Todennäköinen	$1 - 10^{-1}$	Matala riski	Keskinkertainen riski	Korkea riski	Korkea riski
Satunnainen	$10^{-1} - 10^{-2}$	Matala riski	Matala riski	Korkea riski	Korkea riski
Vähäinen	$10^{-2} - 10^{-4}$	Matala riski	Matala riski	Korkea riski	Korkea riski
Epätodennäköinen	$10^{-4} - 10^{-6}$	Vähäpätöinen riski	Matala riski	Keskinkertainen riski	Korkea riski
Hyvin epätodennäköinen	$<10^{-6}$	Vähäpätöinen riski	Vähäpätöinen riski	Keskinkertainen riski	Keskinkertainen riski

Kuva 6. Esimerkki laadullinen/sanallinen riskimatriisista.

2.1.2 Riskianalyysi

Riskianalyysi on IEC 60300-3-9 standardin mukaan jäsennelty prosessi, joka tunnistaa tarkasteltavasta toiminnasta, laitteistosta tai järjestelmästä johtuvien haitallisten seurausten todennäköisyyden ja laajuuden. Haitalliset seuraukset ovat fyysinen vahinko ihmisille, omaisuudelle tai ympäristölle. Riskianalyysi pyrkii vastaamaan kolmeen yleiseen kysymykseen:

- Mikä voi mennä väärin (vaarojen tunnistaminen)?
- Miten todennäköisesti tämä voi tapahtua (taajuusanalyysi)?
- Mitä ovat seuraukset (seurausanalyysi)?

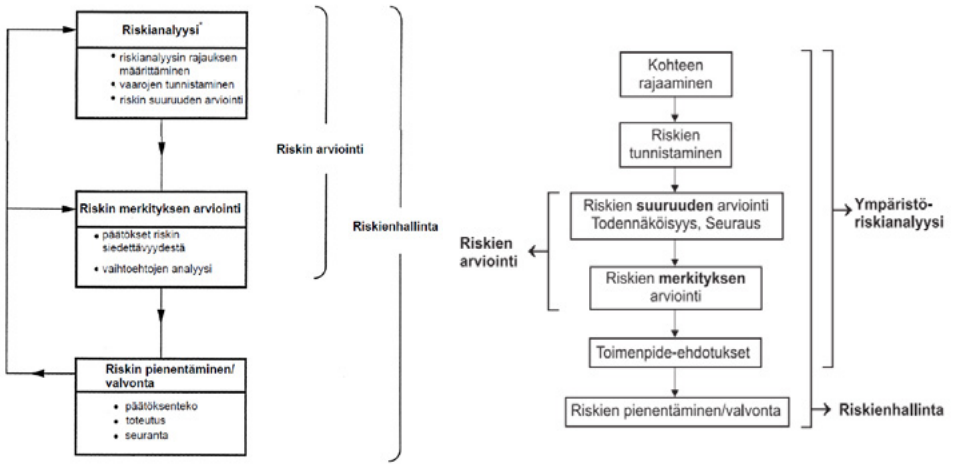
Riski on analysoitava, jotta se voidaan hallita tehokkaasti. Riskin analysointi on tehokas työkalu:

- riskien ja niiden hallintaratkaisuihin liittyvien lähestymistapojen tunnistamiseen,
- tarjoamaan objektiivista tietoa päätöksenteolle, sekä
- lainsäädännön vaatimusten täyttämiseen (SFS-IEC 60300-3-9, 2000).

Arvioidessaan riskin siedettävyyttä ja valitessaan mahdollisia riskin pienentämis- tai välttämistoimenpiteitä voi päätöksentekijä käyttää riskianalyysin tuloksia apuna. Riskianalyysi on osa riskin arviointia ja hallintaprosessia, kuten kuvasta 7 selviää. Se koostuu analyysin rajojen määrittelystä, vaarojen tunnistamisesta ja riskien arvioinnista. Riskianalyysin kokonaistavoite on tarjota rationaalinen (suunnitelmallinen) perusta riskiä koskeville päätöksille.

Nämä päätökset voidaan tehdä osana laajempaa riskienhallintaprosessia vertaamalla riskianalyysin tuloksia siedettävän riskin kriteereihin. Riskianalyysiprosessin toteutusvaiheet ovat seuraavat:

- analyysin rajojen määrittely,
- vaarojen tunnistaminen ja alustava seurausten merkityksen arviointi,
- riskin suuruuden arviointi,
- todentaminen,
- dokumentointi ja
- analyysin päivittäminen (SFS-IEC 60300-3-9, 2000).



Kuva 7. Riskianalyysin ja muiden riskin hallintatoimintojen yksinkertaistettu riippuvuus (SFS-IEC 60300-3-9, 2000) sekä oikealla vertailtavana ympäristöriskianalyysin sisältö. (Wessberg, ym., 2006)

(Wessberg, ym., 2006) mainitsevat YMPÄRI-hankkeen raportissa, että riskianalyysi standardi (SFS-IEC 60300-3-9 2000) kattaa vain riskien suuruuden arvioimiseen asti. Heidän mukaan YMPÄRI-hankkeen tulosten perusteella on asianmukaista tarkastella ympäristöriskianalyysin yhteydessä myös riskin merkityksen arviointia ja riskin pienentämiseen tähtääviä toimia. YMPÄRI-hanke suosittelee ympäristöriskianalyysin sisällöksi oikeanpuoleisen kuvan 7 esitettyä rajausta: Ympäristöriskianalyysi sisältää kohteen rajaamisen, riskien tunnistamisen, riskin suuruuden arvioinnin, riskin merkityksen arvioinnin sekä toimenpide-ehdotukset. Kohteen rajaaminen pitää sisällään analyysin tavoitteiden määrittämisen, analyysin rajaamisen sekä tietojen kokoamisen.

Työturvallisuuslaissa (738/2002) ”*toteutetaan ennalta ehkäiseviä ja suojaavia toimenpiteitä priorisointisuunnitelman mukaisesti, koska kaikkia ongelmia ei todennäköisesti voida ratkaista heti. Lisäksi täsmennetään vastuunjako ja toteutusaikataulu sekä toimenpiteiden toteuttamiseen käytettävät resurssit.” (Työturvallisuuskeskus, 2003)*
Riskianalyysin laadinnan tavoitteet ovat:

- Turvallisuuden hallinta, joka täyttää viranomaisvaatimukset ja varmistaa työpaikan turvallisuus, sekä ennakoi turvallisuus- ja terveysriskit.
- Johtamisen ja uusien hankkeiden suunnittelun tukeminen
- Muutoksen hallinta (Heikkilä;Murtonen;Nissilä;Virolainen;& Hämäläinen, 2007)

Riskianalyysin tavoitteiden määrittelyssä voidaan käyttää seuraavia kysymyksiä:

- Miksi riskianalyysi tehdään?
- Mitä riskianalyysillä on tarkoitus saada aikaan?
- Mitä on valmiina, kun riskianalyysi on saatu valmiiksi?
- Mitä riskianalyysin tekemisestä päättävät analyysilta odottavat? Mihin he tuloksia käyttävät?
- Miten riskianalyysin tekeminen hyödyttää sen tekemiseen osallistuvia henkilöitä? (Heikkilä;Murtonen;Nissilä;Virolainen;& Hämäläinen, 2007)

Kuvassa 8 on esimerkki työturvallisuuskeskuksen laatimasta riskianalyysin yhteenvetolomakkeesta.

Riskianalyysin yhteenvetolomake

Kohde:		Päiväys:		Läsnä:		Sivuja:	
Riski / Vaara	**Riskin syy**	**Pahimmat seuraukset**	**Riskin suuruus**	**Parannusehdotukset**		**Aikataulu ja vastuuhenkilö**	**ok?**
Esim. kompastuminen	- Tavaroita lattialla - Öljy ja vesi	- Kaatuminen - Avainhenkilön sairausloma	4	- Siivous - Järjestyksenpito - Lisää hyllyjä - Öljynimupurua		- N.N. - Kaikki	

Avainsanalista (esimerkkejä):

- Tapaturma: kolhu, viilto, puristuminen, nieluun joutuminen, palohaava, roiske, revähdys
- Fyysinen rasitus: työn raskaus, huono työasento, hankaluus, väsyminen, kuumuus, vetoisuus, pölyisyys, vuorotyö
- Henkinen rasitus: väsyminen, kiire, pakkotahtisuus, yksipuolisuus, viihtyminen, väkivallan uhka, yksinäisyys
- Terveydentila: sairaus, ikä, raskausaika, fyysinen rajoite, lääkkeet, tupakointi, alkoholi, ensiapu
- Palosuojelu: tuli, kipinä, palavat materiaalit, poistumistie, sammutuskalusto, hälytysnumero
- Osaaminen: perehdytys, ohjeet, opasteet, kokemus, koneiden poikkeavat toiminnot

Kuva 8. Työturvallisuuskeskuksen riskianalyysin yhteenvetolomake. (Työturvallisuuskeskus, Riskianalyysin yhteenvetolomake, 2016_b)

2.1.3 Riskien merkityksen arviointi

”Riskien merkityksen arvioinnin tarkoitus on auttaa tekemään päätöksiä riskianalyysin tulosten perusteella siitä, mitä riskejä on tarpeen käsitellä ja mikä on niiden käsittelyn toteuttamisen tärkeysjärjestys.

Riskien merkityksen arviointiin kuuluu analyysiprosessin aikana havaitun riskitason vertaaminen toimintaympäristön määrittelemisen yhteydessä määriteltyihin riskikriteereihin. Tämän vertailun perusteella voidaan päättää riskien käsittelyn tarpeesta.

Päätöksenteossa riski olisi otettava huomioon laaja-alaisesti ja harkittava sellaisten riskien sietotoleranssi, jotka kohdistuvat muihin osapuoliin kuin siihen organisaatioon, joka riskistä hyötyy. Päätökset olisi tehtävä lakien ja viranomaisten vaatimusten sekä muiden vaatimusten mukaan.

Joissain olosuhteissa riskin merkityksen arvioinnin johtopäätöksenä voi olla lisäanalyysin tekeminen. Riskin merkityksen arvioinnin lopputulos voi myös olla päätös olla käsittelemättä riskiä millään muilla tavoin kuin säilyttämällä jo olemassa olevat hallintakeinot. Tähän päätökseen vaikuttaa organisaation asenne riskiin ja sen määrittelemät riskikriteerit.” (SFS-ISO 31000, 2011)

3 Yleisimmät riskianalyysi-menetelmät

Riskianalyysimenetelmiä on useita. Tässä julkaisussa on perehdytty tarkemmin vain osaan analyysimenetelmistä. Turvallisuus on yksi osa tulevaa TPA-menetelmää, joten tässä on huomioita myös turvallisuusanalyysista. Käsite turvallisuusanalyysi tarkoittaa systemaattiseen työskentelyyn perustuvaa analyysiprosessia. Se tähtää tarkasteltavaan kohteeseen sisältyvien vaarojen tunnistamiseen, näiden merkittävyyden arvioimiseen ja hyväksyttävyydestä päättämiseen. Turvallisuusanalyysiin kuuluu myös parannustoimenpiteiden kehittäminen ja niistä päättäminen. (Sarsama;Nissilä;& Lehtinen, 2000)

”Vaarojen ja vaaratilanteiden tunnistamisessa voidaan tarkasteltavasta kohteesta ja tarkastelulle asetetuista tavoitteista riippuen käyttää erilaisia analyysimenetelmiä.” (Sarsama;Nissilä;& Lehtinen, 2000)

Analyysimenetelmät voivat soveltua:

- kokonaisten laitosten ja prosessien tarkasteluun (potentiaalisten ongelmien analyysi (POA), poikkeamatarkastelu (HAZOP)
- rajattujen toimintosarjojen ja työtehtävien tarkasteluun (toimintovirheanalyysi, työn turvallisuusanalyysi)
- rajattujen teknisten järjestelmien tarkasteluun (vika- ja vaikutusanalyysi)
- vakavien onnettomuusmahdollisuuksien yksityiskohtaiseen tutkimiseen (vikapuuanalyysi). (Sarsama;Nissilä;& Lehtinen, 2000)

Onnistunut vaarojen arvioinnin ohjelma vaatii konkreettista johdon tukea, riittävän päteviä ihmisiä, joista osa on koulutettu käyttämään vaarojen arvioinnin tekniikoita, riittävää ajantasaista tietoa ja piirustuksia (PI-kaaviot) kohteesta ja tekniikan/tekniikoiden valinta, jolla analyysi tehdään. Kemian prosessiteollisuudessa on käytössä joustavia vaarojen arvioinnin tekniikoita, jotka sopivat käytettäväksi monenlaisiin tilanteisiin. (Bridges, 2008)

Laadullisia tekniikoita ja menetelmiä, jotka auttavat moniammattilaista tiimiä tunnistamaan mahdollisia onnettomuusskenaarioita ja arvioimaan niitä riittävän yksityiskohtaisesti ovat mm:

- Alustava vaara-analyysi (PreHA)
- Tarkistusluettelot
- SWIFT rakenne « Mitä jos? »
- 2 Guide Word Analysis:
- Poikkeamatarkastelu (HAZOP)
- FMEA ja FMECA (Bridges, 2008).

Muita laadullisia menetelmiä, joita käytetään muissa prosesseissa kuin kemian prosessiteollisuudessa:

- Juurisyiden analyysi (yksittäis-vahinkoanalyysi) (RCA)
- Skenaarioanalyysi
- Liiketoiminta-analyysi (BIA)
- Syy ja vaikutusanalyysi
- Yllätyspiirien analyysi
- Vaara-analyysi ja kriittiset tarkistuspisteet (HACCP)
- Ohjattu haastattelu ja aivoriihi
- Delfoi tekniikka (SFS-EN 31010, 2013)

Kun skenaariot on tunnistettu, laadullinen vaaratarkastelu voidaan analysoida tarkemmin käyttämällä yhtä tai useampaa määrällistä menetelmää. Määrälliset menetelmät eivät yksilöi mahdollisia onnettomuuksia, mutta ne sen sijaan tukevat tai auttavat tekemään tilastollisia arviointeja tietyistä skenaarioista.

- LOPA (Kerrossuojausanalyysi)
- Myrkyllisten aineiden riskinarviointi
- Vikapuuanalyysi (FTA)
- Tapahtumapuuanalyysi (ETA)
- Ihmisen luotettavuus -analyysi (HRA) (Bridges, 2008).

Muita menetelmiä ovat mm:

- Syy ja seurausanalyysi
- Markov-analyysi
- Monte Carlo analyysi
- Bayes-analyysi
- Toimintavarmuuskeskeinen kunnossapito (RCM). (SFS-EN 31010, 2013)

3.1 RCM – LUOTETTAVUUSKESKEINEN KUNNOSSAPITO

RCM tulee sanoista Reliability Centered Maintenance, eli luotettavuuskeskeinen kunnossapito. Nimi sisältää koko menetelmän idean, eli laitteen kunnossapito ja varsinkin ennakoiva kunnossapito suunnitellaan laitteen luotettavuuden perusteella. RCM:n juuret juontuvat amerikkalaisesta ilmailuteollisuudesta alkaen 1960-luvun lopulta (SFS-EN 60300-3-11:en, 2015). Siihen mennessä ennakoiva ja varsinkin ehkäisevä kunnossapito oli jo muodostunut lentokoneiden lentoturvallisuuden ja luotettavuuden kivijalaksi. Tuohon aikaan ehkäisevä toiminta perustui vahvasti vikaantumisriskien ehkäisemiseen suorittamalla huoltotoimenpiteet ennalta määrätyn ajanjakson, lentotuntimäärän tms. perusteella. Tämä johti melko nopeasti tilanteeseen, jossa ylihuollon määrä kasvoi. Tällöin oli vielä vallalla uskomus, että hallitseva vikaantumismekanismi olisi loppuun kuluminen tai muu rasitukseen perustuva (Mäki, 2016). Amerikkalaiset alan uranuurtajat Nowlan ja Heap tekivät mittavia tutkimuksia niin lentokoneiden, laivojen kuin teollisuudenkin laitteiden parissa. He havaitsivat, että vain noin 10–20 % kaikista vikaantumismekanismeista noudatti tätä nk. kylpyammekäyrä- mekanismia (Nowlan & Heap, 1978). Vanha uskomus johti helposti kalliiseen ”ylihuoltoon”, jollaista varsinkin lentokoneiden ”varman päälle filosofia” noudatti. Toinen merkittävä havainto oli, että määräaikaishuoltotoimenpiteet, joissa ehjä laite avattiin, vaihdettiin tai muuten huollettiin, johti vikaantumisen kasvuun johtuen inhimillisten virheiden tms. johdosta. RCM- menetelmä kehittyi tästä havainnosta kohti tilannetta, jossa pyrittiin selvittämään kohteen todellinen vikaantumisprofiili. Tieto, että suurin osa vikaantumisista olisi enemmän tai vähemmän satunnaisia, johti kuntoon perustuvan kunnossapidon kehittymiseen. Toinen merkittävä havainto oli ymmärtää, mikä on kunkin laitteen kriittisyys järjestelmän luotettavuuden ja turvallisuuden kannalta. (Mäki, 2016)

3.1.1 RCM- menetelmän keskeinen sisältö

Koska RCM:n tavoite on laatia tarkoituksen mukainen ja kustannustehokas ennakoivan kunnossapidon suunnitelma, on ensimmäinen tehtävä päättää, mille tasolle analyysi on tehtävä. Teollisuudessa tyypillinen analyysin aloitustaso on tehtaan tai laitoksen koneiden toimintopaikkataso. Toimintopaikka on toiminnallisen kokonaisuuden ”osoite”, ja se sisältää laitteet ja vastaavat, jotka ko. toiminnon mahdollistavat. Toimintopaikkoja on tyypillisesti isossa tehtaassa useita satoja tai jopa useita tuhansia. Toimintopaikat tulee ensin asettaa tärkeysjärjestykseen, mikä RCM:ssä tehdään kriittisyysanalyysin avulla (SFS-EN 60300-3-11:en, 2015). Kriittisyysanalyysissä arvioidaan ko. toimintopaikan vikaantumisen merkitys tehtaan tuotannolle, turvallisuudelle, laaduntuottokyvylle sekä kunnossapitokustannuksille. Jos tehdas tai kone on jo ollut käytössä, voidaan arviointiin ottaa mukaan ko. toimintopaikan luotettavuus, eli kuinka ”vikaherkkä” ko. toiminto on? Näiden kahden kriteerin, vian vaikutuksen ja vian todennäköisyyden perusteella määräytyy kohteen kriittisyysindeksi. Tyypillisesti jaottelu pelkistetään luokkiin A, B ja C, joista A tarkoittaa kaikkein kriittisintä luokkaa, B keskikriittisistä ja C vähiten kriittistä. Nyrkkisääntönä käytetään yleensä

ajatusta, että A- kriittisiä kohteita on n. 20-30 % kaikista toimintopaikoista. B- kriittisten osuus on teollisuudenalasta riippuen 30- 40 % ja loput ovat C- kriittisiä. (Moubray, 1997)

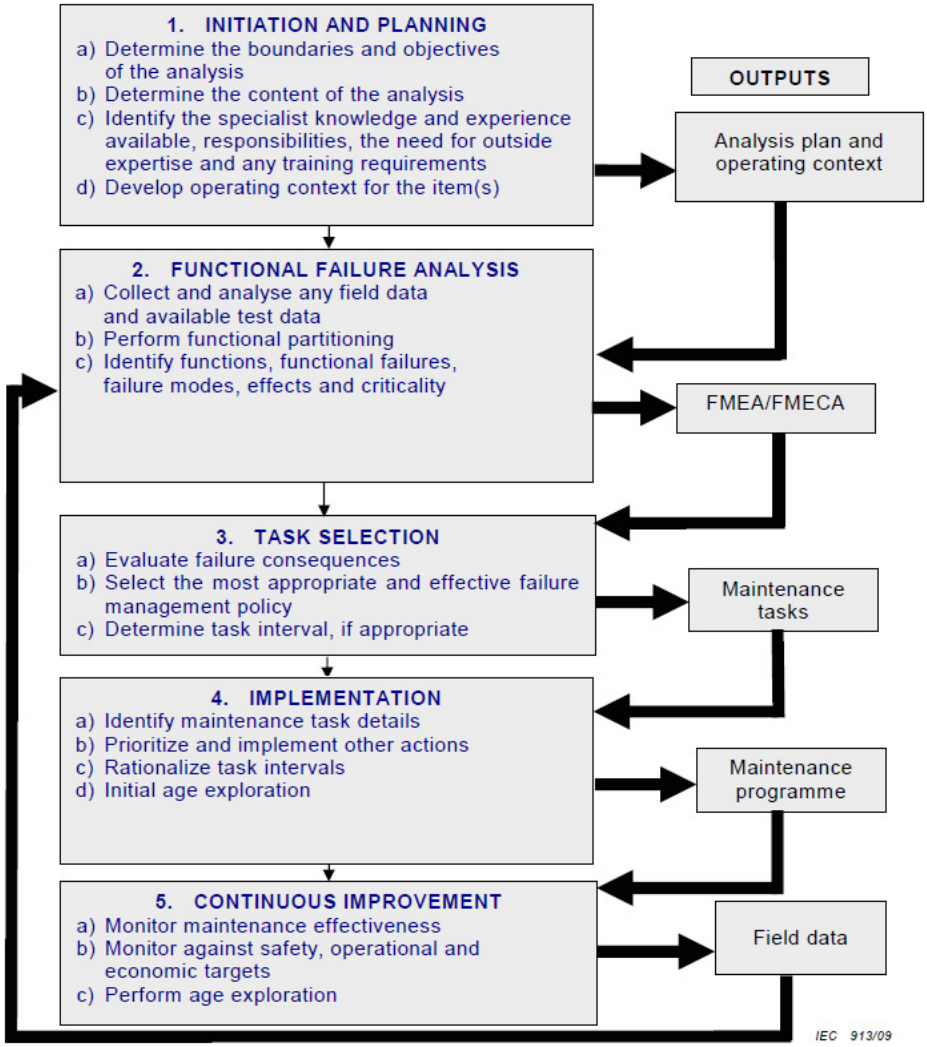
RCM:ssä jatketaan A-kriittisten kohteiden analysoimista sen suhteen, miten ne voivat vikaantua, mistä syystä ja kuinka usein. Tähän vaiheeseen käytetään yleensä nk. vika- vaikutus- ja kriittisyysanalyysiä (Failure Mode, Effect and Criticality Analysis). Tässä analyysissä keskeisiä kysymyksiä ovat:

1. Mitkä ovat ko. toimintopaikan toiminnot?
2. Mitkä ovat toimintojen todennäköisimmät häiriötilanteet eli toiminnalliset viat?
3. Mitkä vikamuodot eli syyt voivat johtaa ko. häiriöihin ja
4. Mikä on kunkin vikamuodon vaikutukset järjestelmän toimintaan ja turvallisuuteen sekä kustannuksiin?

Kohdassa 3 voidaan tarpeen mukaan määrittää vielä vikamuotojen syitä ja mekanismeja sen mukaan, mikä on tarkoituksenmukaista lopputuloksen kannalta. Vika- ja vaikutusanalyysin jälkeen on kohteen potentiaalisemmat vikamuodot tunnistettu ja laitettu järjestykseen. (Mäki, 2016)

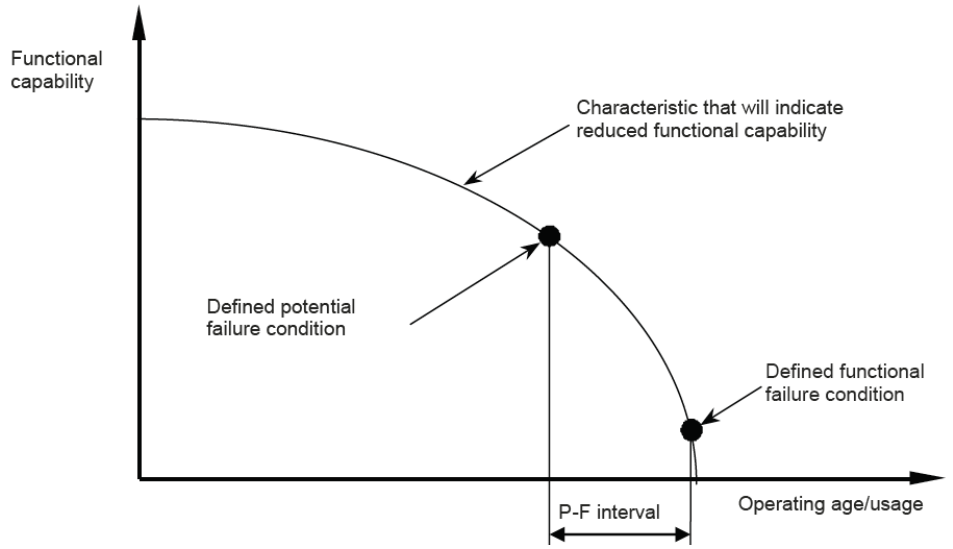
RCM- analyysin lopputulos eli syntynyt huoltosuunnitelma määritetään vika- ja vaikutusanalyysin perusteella. Kunkin vikamuodon kohdalla pyritään määrittämään joko ennakoiva, ehkäisevä tai parantava toimenpide, jolla ko. vikamuodon riskiä voidaan pienentää. Ennakoiva toimenpide tarkoittaa sitä, että vikamuodon synnystä saadaan ajoissa indikaatio, jonka perusteella varsinainen korjaava toimenpide voidaan määrittää ja ajoittaa kustannustehokkaimmin. Ennakoiva toimenpide on tyypillisesti käyttäjien suorittama visuaalinen tarkastus tai kunnonvalvonnan mittaus. Ehkäisevän toimenpiteen tarkoitus on estää vikamuodon synty. Tyypillisiä toimenpiteitä ovat mm. voitelu, puhdistus, kuluvien osien vaihto tms. Parantava toimenpide on luonteeltaan kertaluontoinen, kuten esim. käyttöohjeen täsmennys, lisäkoulutus, laitteen modernisointi tai muu muutos, jolla vikamuodon synty estetään kokonaan. Jos mitään edellä mainituista toimenpiteistä ei pystytä riittävän selkeästi määrittämään, voidaan päätyä nk. Run To Failure- päätökseen (RTF), mikä tarkoittaa vikaantumisriskin hyväksymistä. Tällöin on tärkeää varmistua korjausprosessin tehokkuuteen ja varaosien saatavuuteen. Jos vian vaikutus on pieni, voidaan analyysissä päätyä myös RTF- vaihtoehtoon. Jos vikamuodon tai sen vaikutuksen todetaan olevan luonteeltaan piilevä, eli se ei ilmene normaalissa toiminnassa, päädytään erilliseen Failure Finding- toimenpiteeseen. Tämä tarkoittaa testaustoimintaa, jossa ko. toiminnon kunto todetaan. Nämä toimenpiteet ovat tyypillisiä kahdennetuille järjestelmille sekä suoja- ja varojärjestelmille. (Mäki, 2016)

Kuvassa 9 on esitettynä RCM prosessin kulku SFS-EN 60300-3-11:en standardin mukaisesti.



Kuva 9. RCM prosessin kulku (SFS-EN 60300-3-11:en, 2015) standardin mukaan

Huoltotoimenpiteiden toistovälin määrittämisessä on ennakoivien toimenpiteiden osalta pyrittävä tunnistamaan kuvassa 10 esitetty nk. P-F- aika (Potential Failure-Functional Failure). Se tarkoittaa sitä ajanjaksoa, kauanko vikamuodon alkuhetkestä kuluu aikaa siihen, että ko. toiminto voidaan menettää. Tähän aikajaksoon tulisi määrittää vähintään kaksi tarkistus- tai mittauspistettä. Ehkäisevässä toimenpiteessä tulisi tunnistaa vikamuodon keskimääräinen esiintymisväli, eli Mean Time To Failure (MTTF). Toimenpide tulee ajoittaa riittävän aikaiseksi tähän arvoon verrattuna.



Kuva 10. P-F ajanjakso (SFS-EN 60300-3-11:en, 2015)

3.1.2 RCM- menetelmän onnistumisen edellytyksiä

RCM- analyysin onnistuminen riippuu paljolti siitä, kuinka hyvin kohdejärjestelmän vikaantumisriskien tilannekuva saadaan kuvattua. RCM- analyysiryhmässä tulee olla edustus kohteen käyttäjien ja kunnossapitäjien lisäksi hyvä ymmärrys tuotannon kustannusvaikutuksista sekä teknisesti ajatellen kohteen erityisvaatimuksista. Normaalisti analyysi suoritetaan nk. neuvotteluhuoneistuntona, mutta tarpeen tullen analyysi voidaan siirtää myös tapahtuvaksi kentällä kohteen välittömässä läheisyydessä. Analyysi vaatii hyvää keskittymistä, joten yhden istunnon kesto ei saa ylittää neljää tuntia. Analyysillä pitää olla asiansa osaava vetäjä, eli nk. fasilitaattori. Hänen tehtävänään on pitää huolta, että analyysi etenee suunnitelman mukaan ja siinä noudatetaan RCM:n periaatteita. (Mäki, 2016)

Analyysin sujuva dokumentoiminen on eräs onnistumisen kulmakivi. RCM:n läpivientiin on olemassa useita kaupallisia ohjelmistotyökaluja, joissa on mukana tarvittavat toiminnallisuudet itse analyysin vaiheiden dokumentointiin sekä mahdollisiin luotettavuusmatemaattisiin tarkasteluihin. Analyysi voidaan dokumentoida myös esim. Excel- lomakkeella. (Mäki, 2016)

Ennen kuin analyysi aloitetaan, on ensiarvoisen tärkeää selvittää, mikä on analysoitavan järjestelmän nykytila mitattuna esim. käyttövarmuuden mittareilla. Näitä ovat esim. käytettävyys, suunnittelemattomien seisokkien tai häiriöiden osuus, tuotantotehokkuus tai kokonaiskustannukset. Kun analyysi on tehty ja saadut toimenpidesuositukset on viety käytäntöön, voidaan näillä samoilla mittareilla todentaa analyysin tuottama hyöty. Tämä hyötynäkökulma on ensiarvoisen tärkeää, jotta menetelmä on uskottava ja sen tulokset synnyttävät tarvittavan motivaation jatkaa systemaattista analyyttistä kehittämistä esim. muihin kohteisiin. (Mäki, 2016)

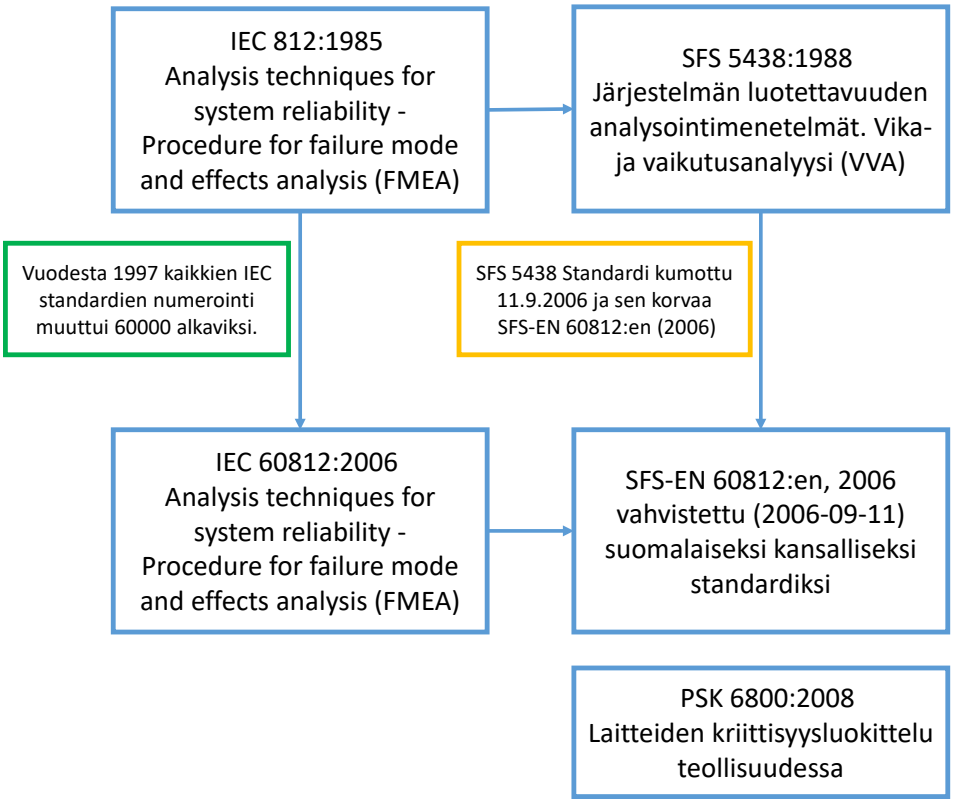
3.2 VIKA-, VAIKUTUS- JA KRIITTISYYSANALYYSI

Vika- ja vaikutusanalyysi, (lyh. VVA, engl. Failure Mode and Effects Analysis, FMEA) ja vika-, vaikutus- ja kriittisyysanalyysi, (lyh. VVKA, engl. Failure mode, effects, and criticality analysis, FMECA) ovat toimintavarmuuden analysointimenetelmiä. Ne ovat tarkoitettu sellaisten vikojen tunnistamiseen, joiden seurauksilla on merkittävä vaikutus tarkasteltavan järjestelmän suorituskykyyn. (SFS-EN 60812:en, 2006)

Haettaessa tietoa tämän raportin kirjoittamiseen, ilmeni (mm. opinnäytetöiden kautta), että Suomessa VV-analyysit tehdään kahteen standardiin pohjautuen; vuonna 2006 kumottuun SFS 5438 ja laitteiden kriittisyystarkasteluun PSK 6800 standardiin. Osa yrityksistä käyttää SFS-EN 60812en:2006 ” Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)” standardia, jossa annetaan ohjeita ja esimerkkejä vika- ja vaikutusanalyysin sekä vika-, vaikutus ja kriittisyysanalyysin tekemiseen. Standardia SFS-EN 60812en:2006 ei ole vielä käännetty suomeksi. Se on saatavana Suomen standardoimisliiton kautta englanninkielisenä. Raportin kirjoittamisen aikana huomioitiin myös, että uusimmissa kansainvälisissä tieteellisissä julkaisuissa puhuttaessa FMEA:sta, käytettiin lähteenä IEC 60812:2006 standardia.

Alla olevassa kuvassa 11 on hieman selkeytetty standardiasiaa. Vuodelta 1988 oleva suomalainen SFS 5438 standardi on suora käännös kansainvälisestä IEC 812:1985 standardista. Vuodesta 1997 kaikkien IEC standardien numerointi muuttui 60000 alkaviksi (IEC, 2016), jolloin standardien asiasisältö pysyi samana, mutta esim IEC 812:stä tuli IEC 60812. Em. standardin versiomuutos tapahtui 2006 ja tärkeimmät muutokset vanhaan versioon verrattuna olivat:

- Johdanto vikamuotojen vaikutuksiin ja kriittisyysluokitteluihin
- Sisällytetty laajasti autoteollisuudessa käytettävät menetelmät
- Lisätty viittauksia ja liityntöjä toisiin vikamuotojen analyysi menetelmiin
- Lisätty esimerkkejä
- Opastusta eri FMEA menetelmien hyötyihin ja haittoihin (SFS-EN 60812:en, 2006).



Kuva 11. Kriittisyysanalyysistandardien päivitykset

Edellä mainittuja toimintavarmuuden analysointimenetelmiä ja standardeja, sekä kumottuja että nykyisiä, avataan hieman enemmän seuraavissa alakappaleissa, koska ne liittyvät TPA menetelmän kehitykseen ja sisältöön.

3.2.1 VVA

VVA perustuu alimmalle komponentti- tai osajärjestelmätasolle, jolle voidaan määrittää vioittumiskriteerit eli ensisijaiset vioittumistavat. Peruselementtien vikaantumisominaisuuksiin ja järjestelmän toiminnalliseen rakenteeseen perustuva VVA määrittää elementtien vikojen ja järjestelmän vikojen, toimintahäiriöiden, käyttörajoituksien ja suorituskyvyn huonontumisen välisen yhteyden. (SFS 5438, 1988). Yleensä sarakkeisiin kerätään tietoja:

- Tutkittavan järjestelmän osan nimi (laite)
- Järjestelmän osan tehtävä
- Järjestelmän osan tunnus
- Vioittumistavat
- Vian aiheuttaja (vioittumissyyt)
- Vian vaikutukset
- Vian havaitsemistavat
- Laadullinen arvio vian merkittävyydestä ja vaihtoehtoiset varokeinot
- Huomautukset (SFS 5438, 1988)

Kun tarkastelua tehdään VVA menetelmällä, se on pääasiassa laadullinen eli sanallisesti arvioitu ja tästä esimerkki taulukossa 4.

Taulukko 4. Esimerkki riskinarviointimenetelmästä ja tekniikasta; vika- ja vaikutusanalyysi taulukosta kuvitetulla esimerkkitapauksella. (Suutama, 2015)

Laite	Tehtävä / toiminto	Toiminnallinen vikaantuminen	Vikaantunut komponentti / vikamuoto	Vian aiheuttaja, tarkempi kuvaus viasta	Vian vaikutus		Havaitsemistavat	Korjaustyön kuvaus (aika, työvoima ja kustannukset)
					Paikalliset vaikutukset	Seuraukset muuhun prosessiin		
Pumppu 1	Nesteen pumppaus	Ei tuotantoa	Juoksupyörä	Irtoaminen, kuluminen	Voi vaurioittaa pesää	Osaprosessi ei käytettävissä	Kunnonvalvonta, toiminnon heikentyminen	Pumpun huolto, 8 h, 2 asentajaa 3000 €
			Laakerointi	Hajoaminen, huono linjaus	Akselin vaurioituminen	Osaprosessi ei käytettävissä	Kunnonvalvonta	Laakeroinnin vaihto, 4 h, 2 asentajaa, 1500 €
			Moottori	Ylikuumeneminen	Tulipalovaara, turvallisuusriski	Osaprosessi ei käytettävissä	Kunnonvalvonta	Moottorin vaihto, 4 h, 2 asentajaa, 1000 €
	Neste ei saa vuotaa	Vuoto	Putkivuoto	Täriná	Turvallisuusriski	Ei seurauksia muuhun prosessiin	Visuaalinen havainto	Putken hitsaus, 4 h, 2 ulkop. asentajaa, 800 €

VVA:ta on tarpeen täydentää muilla menetelmillä, erityisesti silloin kun tutkitaan moninkertaisia vikoja ja niiden seurausvaikutuksia. (SFS 5438, 1988) Alla on lueteltuna menetelmien hyviä puolia:

- VVA on erityisen tehokas, kun sitä sovelletaan osiin, jotka aiheuttavat koko järjestelmän vikaantumisen. (SFS 5438, 1988).
- VVA:lla voidaan tunnistaa myös komponentteja, joihin inhimilliset tekijät vaikuttavat erittäin herkästi. Kuitenkin näiden vaikutusten huomioon ottaminen vaatii järjestelmän eri komponenttien ominaisuuksien tai toiminnan perinpohjaista tuntemusta. (SFS 5438, 1988).

3.2.2 VVKA

Kun edellä kuvattua VVA:ta täydennetään vian esiintymistodennäköisyydellä ja vian kriittisyystasolla, saadaan vika-, vaikutus- ja kriittisyysanalyysi eli VVKA (SFS 5438, 1988).

Taulukko 5. Esimerkki vika-, vaikutus- ja kriittisyysanalyysilomakkeesta mukaillen standardia SFS5438 (SFS 5438, 1988)

Laite	Tehtävä	Vioittumistapa	Vian aiheuttaja	Vian vaikutus		Vian havaitsemistavat	Vaihtoehtoisia varokeinoja tai parannusehdotuksia	Kriittisyysarvo/ max.kriittisyysarvo	Huom!
				Paikalliset vaikutukset	Vaikutukset koko järjestelmän toimintaan				

VVA:ssa ja VVKA:ssa pieni eroavaisuus löytyy kriittisyysarvioinnissa. VVA-lomakkeella vian vaikutuksen luokittelu kriittisyyden perusteella ilmaistaan yksinkertaisesti vain laitteen kriittisyystasoilla I-IV. Kriittisyystaso arvioidaan tapahtumalla, joka toteuttaa tietyn kriittisyysehdon. Kriittisyydenarviointi voidaan tehdä käyttämällä kriittisyysmatriisia, josta esimerkki alla olevassa taulukossa 6. (SFS 5438, 1988)

Taulukko 6. Kriittisyysmatriisi (SFS 5438, 1988)

	Kriittisyys-tasot				
Tapahtuma, joka saattaa aiheuttaa järjestelmän ensisijaisen toimintatavan puuttumisen johtaen järjestelmän tai sen ympäristön huomattaviin vahinkoihin ja kuolemantapauksiin ja muuten vakaviin henkilövahinkoihin.	**IV**				
Tapahtuma, joka saattaa aiheuttaa järjestelmän ensisijaisen toimintatavan puuttumisen johtaen järjestelmän tai sen ympäristön huomattaviin vahinkoihin ja kuolemantapauksiin ja muuten vakaviin henkilövahinkoihin.	**III**				
Tapahtuma, joka saattaa aiheuttaa järjestelmän ensisijaisen toimintatavan puuttumisen johtaen järjestelmän tai sen ympärsitön huomattaviin vahinkoihin, mutta vähäpätöisiin henkilövahinkoihin.	**II**				
Tapahtuma, joka huonontaa järjestelmän suorituskykyä, mutta ei vahingoita järjestelmää merkittävästi eikä aiheuta huomattavia henkilövahinkoja.	**I**				
		hyvin pieni	pieni	keski-suuri	suuri
	vian esiintymistodennäköisyys				

Kriittisyysmatriisi osoittaa hyvin kriittisyyden tason (piste sijaitsee kaksiulotteisen koordinaatiston pisteessä) ja vian esiintymistodennäköisyyden (vaakasuora x akseli). Taulukon esimerkissä esiintymistodennäköisyydet tai – taajuudet on jaettu mielivaltaisesti neljään luokkaan: hyvin pieni, pieni, keskimääräinen, suuri. Monissa tapauksissa esiintymistodennäköisyydet tai – taajuudet luokitellaan epälineaarisesti. Kun vioittumistavat on luokiteltu ja niille on määrätty esiintymistodennäköisyys/-taajuus, ne laitetaan sille kuuluvaan ruutuun matriisissa. Mitä kauempana ruutu on origosta (lävistäjän suuntaan), sitä suurempi on kriittisyysarvo ja sitä kiireellisimmin tarvitaan korjaavia toimenpiteitä. Jokaista kriittisyysanalyysia varten pitää määrittää erityiset esiintymistodennäköisyyksien tai -taajuuksien alueet. (SFS 5438, 1988)

3.2.3 FMEA/FMECA

Suomalaiseksi kansalliseksi standardiksi vahvistetun SFS-EN 60812:2006 mukaan riskianalyysimenetelmät FMEA:n ja FMECA:n täydentävinä menetelminä ovat seuraavat riskienhallinnan standardit:

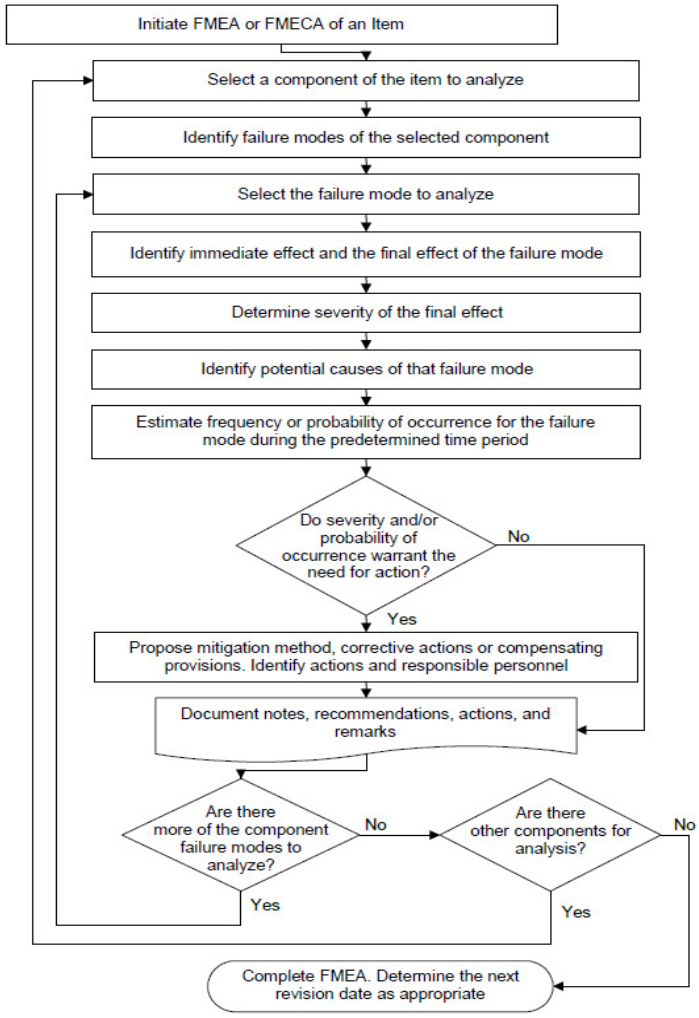
- IEC 60300-3-1:2003, Dependability management – Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology,
- IEC 61025, Fault tree analysis (FTA),
- IEC 61078, Analysis techniques for dependability – Reliability block diagram and Boolean methods

Riskien hallinta ja riskien arviointimenetelmät SFS-EN31010 standardin mukaan FMEA on tekniikka, joka tunnistaa vikamuodot ja – mekanismit ja niiden vaikutukset. Itse menetelmää ja sen käyttöä ohjeistaa parhaiten SFS-EN 60812:en:2006 "Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)" Kuvassa 12 on havainnollistettu FMEA/FMECA analyysin kulku (SFS-EN 60812:en, 2006)

On olemassa useita erilaisia FMEA tyyppejä:

- Suunnittelu tai tuote FMEA (komponentit ja tuotteet),
- järjestelmä FMEA (järjestelmät),
- prosessi FMEA (valmistus- ja kokoonpanoprosessit),
- palvelu FMEA,
- ohjelmisto FMEA.

FMEA/FMECA -analyysejä voidaan soveltaa fyysisen järjestelmän suunnitteluun, valmistukseen ja testaukseen. (SFS-EN 31010, 2013); (SFS-EN 60812:en, 2006)



Kuva 12. FMEA/FMECA analyysin kulku. (SFS-EN 60812:en, 2006)

”FMECA tutkimuksen tuotos sisältää tärkeysluokituksen, joka perustuu järjestelmän vikaantumistodennäköisyyteen, vikaantumismuodon aiheuttamaan riskitasoon tai riskitason ja vikaantumismuodon ’havaittavuuden’ yhdistelmään. FMECA voi antaa määrällisen tuotoksen, jos käytetään sopivia vikaantumistiheystietoja ja määrällisiä seurauksia.” (SFS-EN 31010, 2013).

Kriittisyysanalyysin tarkoituksena on kategorisoida vikamuodot niiden aiheuttamien vaikutusten vakavuuksien (severity=S), esiintymistodennäköisyyksien (occurrence=O) ja havaitsemiseen (detection=D) liittyvien tietojen pohjalta. (Ramentor Oy, 2011)

Alla olevissa taulukoissa 7-9 on esimerkkejä autoteollisuudessa käytetyistä vian vakavuus-, esiintymistodennäköisyyksien- sekä havaitsemisluokituksista. (SFS-EN 60812:en, 2006)

Taulukko 7. Esimerkki autoteollisuudessa käytetystä vian vaikutuksen vakavuusluokituksesta SAE J1739 mukaan. (SFS-EN 60812:en, 2006)

Severity	Criteria	Ranking
None	No discernible effect.	1
Very minor	Fit and finish/squeak and rattle item does not conform. Defect noticed by discriminating customers (less than 25 %).	2
Minor	Fit and finish/squeak and rattle item does not conform. Defect noticed by 50 % of customers.	3
Very low	Fit and finish/squeak and rattle item does not conform. Defect noticed by most customers (greater than 75 %).	4
Low	Vehicle/item operable but comfort/convenience item(s) operable at a reduced level of performance. Customer somewhat dissatisfied.	5
Moderate	Vehicle/item operable but comfort/convenience item(s) inoperable. Customer dissatisfied.	6
High	Vehicle/item operable but at a reduced level of performance. Customer very dissatisfied.	7
Very high	Vehicle/item inoperable (loss of primary function)	8
Hazardous with warning	Very high severity ranking when a potential failure mode affects safe vehicle operation and/or involves non-compliance with government regulation with warning.	9
Hazardous without warning	Very high severity ranking when a potential failure mode affects safe vehicle operation and/or involves non-compliance with government regulation without warning.	10

Taulukko 8. Esimerkki vikamuodon esiintymistodennäköisyys luokituksesta. (SFS-EN 60812:en, 2006)

Failure mode occurrence	Rating, *O*	Frequency	Probability
Remote: Failure is unlikely	1	≤ 0,010 per thousand vehicles/items	$\leq 1x10^{-5}$
Low: Relatively few failures	2	0,1 per thousand vehicles/items	$1x10^{-4}$
	3	0,5 per thousand vehicles/items	$5x10^{-4}$
Moderate: Occasional failures	4	1 per thousand vehicles/items	$1x10^{-3}$
	5	2 per thousand vehicles/items	$2x10^{-3}$
	6	5 per thousand vehicles/items	$5x10^{-3}$
High: Repeated failures	7	10 per thousand vehicles/items	$1x10^{-2}$
	8	20 per thousand vehicles/items	$2x10^{-2}$
Very high: Failure is almost inevitable	9	50 per thousand vehicles/items	$5x10^{-2}$
	10	≥100 in thousand vehicles/items	$\geq 1x10^{-1}$

Taulukko 9. Esimerkki vikaantumisen todennäköisyydestä ja miten vikamuotojen havaitsemiset luokitellaan. (SFS-EN 60812:en, 2006)

Detection	Criteria: Likelihood of detection by Design Control	Ranking
Almost certain	Design Control will almost certainly detect a potential cause/mechanism and subsequent failure mode	1
Very high	Very high chance the Design Control will detect a potential cause/mechanism and subsequent failure mode	2
High	High chance the Design Control will detect a potential cause/mechanism and subsequent failure mode	3
Moderately high	Moderately high chance the Design Control will detect a potential cause/mechanism and subsequent failure mode	4
Moderate	Moderate chance the Design Control will detect a potential cause/mechanism and subsequent failure mode	5
Low	Low chance the Design Control will detect a potential cause/mechanism and subsequent failure mode	6
Very low	Very low chance the Design Control will detect a potential cause/mechanism and subsequent failure mode	7
Remote	Remote chance the Design Control will detect a potential cause/mechanism and subsequent failure mode	8
Very remote	Very remote chance the Design Control will detect a potential cause/mechanism and subsequent failure mode	9
Absolutely uncertain	Design Control will not and/or cannot detect a potential cause/mechanism and subsequent failure mode; or there is no Design Control	10

Riskianalyysin lopputuloksena vikamuodoille muodostuu ns. riskiluku (Risk Priority Number, RPN) kuvaamaan vikamuodon merkittävyyttä. Riskiluku muodostuu vikojen vakavuuksien, esiintymistodennäköisyyksien ja havaitsemisen antamasta tulosta. Mitä suurempi riskiluku on, sitä merkittävämpi vikamuoto on. Riskianalyysin avulla saadaan selville ne vikamuodot, joille ensisijaisesti tulisi löytää parantavia toimenpiteitä vikamuodon esiintymistodennäköisyyden, vaikutusten pienentämiseksi tai havaittavuuden parantamiseksi. (Ramentor Oy, 2011)

Yllä mainittuihin taulukoihin liittyen, joitakin puutteita RPN:ssa on havaittu standardin SFS-EN 60812:en, 2006 mukaan esimerkiksi:

- Erot vaihteluväleissä: 88 % vaihteluvälistä on tyhjä, vain 120 arvoa tuhannesta on käytössä
- Päällekkäiset/samat RPN arvot: useita yhdistelmiä, joissa eri tekijät johtavat samaan RPN:ään
- Laskenta (SxOxD=RPN) on herkkä pienille muutoksille; yhden tekijän pienelläkin muutoksella on paljon suurempi vaikutus silloin, kun tekijät ovat suurempia kuin ne olisivat pieniä, esimerkiksi:
  - Suuret tekijät: 9x9x3 = **243** verrattuna 9x9x4 = **324**
  - Pienet tekijät: 3x4x3 = **36** verrattuna 3x4x4 = **48**
- Puutteellinen tai riittämätön skaalaus; esiintymistodennäköisyyksien taulukko (esim. taulukko 9) ei ole suhteessa tai lineaarinen esim. luku voi olla 2,5 tai 2, kahden peräkkäisen **seuraus**luokituksen välillä

- Puutteellinen RPN alue; erot RPN lukujen välillä saattavat olla vähäisiä, vaikka se tosiasiassa on merkittävä. Esimerkki arvoista:
  - ***1.*** S = 6, O = 4, D = 2, tuottaisi RPN = **48**, kun taas
  - ***2.*** S = 6, O = 5, ja D = 2 tuottaisi RPN = **60**.
  - Toinen RPN luku ei ole kaksinkertainen ensimmäiseen RPN lukuun verrattuna, vaikka se tosiasiassa pitäisi taulukon 9 (esiintymistodennäköisyys) mukaan olla, koska
    - Luokitus 4 = 1 tuhannesta ajoneuvosta/laitteesta $1x10^{-3}$
    - Luokitus 5 = 2 tuhannesta ajoneuvosta/laitteesta $2x10^{-3}$
  - Siksi RPN numeroita ei pidä verrata suoraviivaisesti.
- RPN lukua tuijottamalla voidaan tehdä harhaanjohtavia päätelmiä, jos asteikot ovat järjestyksessä, mutta eivät järkevästi. (SFS-EN 60812:en, 2006)

Taulukko 10. Esimerkki riskianalyysistä (Karjalainen, 2016)

QUALITY KNOWHOW KARJALAINEN OY — PFMEA

PFMEA -kohde / tuote	Ruiskuvalu	**Suunnitteluvastuu**	JJX	**FMEA**	1
Alaprosessi	-	**FMEA-vastuu**	JJX	**Laatijat**	JJX/ OUPV AUPV PPP
Prosessidokumentti	Prost_05	**Tavoite pvm.**	1.1.2005	**Pvm / rev.**	1.1.2005
Prosessivastaava	JJX	**Yht.henk.**	JJX	**Toimenpiderajа**	>90

RPN= VA (vaikutus) * ES (esiinnyminen) * LÖ (löydettävyys) — TOIMENPITEIDEN TULOKSET

Prosessivaa nimi/ osaerof tarkoitus	Vikamuoto	Vian aiheuttamat seuraukset	V A	LE	Vian mahdolliset syntymissyyt	E S	Nykyinen menettelp/ seurantaf valvonta	LÖ	RPN	Toimenpiteet	Vastuuhlöt	Aikataulu	OK pvm.	V A	E S	LÖ	RPN
1 Ruiskutus, Sisäiset ruiskutus kanavat	Vajaa kappale	Epätasainen täyttö	8		Ruiskutuspistee n sijainti	1	Silmämääräinen	2	16					8			0
	Vääntyily	Istuu huonosti kanteen	6		Epätasainen seinän vahvuus	2	Silmämääräinen/ Mittaus	4	48					6			0
	Yhtymäsauma	Yhtymäsauma näkyvällä pinnalla	8		Ruiskutuspistee n sijainti	1	Silmämääräinen	2	16					8			0
		Yhtymäsauma näkyvällä pinnalla	8		Kanavatyyppi	1	Silmämääräinen	5	40					8			0
		Yhtymäsauma näkyvällä pinnalla	8		Kanavakoko	1	Silmämääräinen	5	40					8			0
		Yhtymäsauma näkyvällä pinnalla	8		Muottilämpötila	5	Silmämääräinen	4	160	Valvontalaite	Antti	1.2.2005	28.1.	8	2	4	64
		Yhtymäsauma näkyvällä pinnalla	8		Pl-a lämpötila	5	Silmämääräinen	4	160	Valvontalaite	Antti	1.2.2005	29.1.	8	2	4	64
		Yhtymäsauma näkyvällä pinnalla	8		Ruiskutusnope us	3	Silmämääräinen	3	72	Prosessin valvonta	Antti	1.2.2005	26.1.	8	2	3	48
	Ruiskutusjälj et	Kuutamo	9		Ruiskutuspistee n sijainti	5	Silmämääräinen	3	135	Portin suurennus	Eero	1.2.2005	30.1.	9	2	3	54
		Jetting	5		Ruiskutuspistee n sijainti	3	Silmämääräinen	3	45					5			0

FMEA-analyysissä edetään riskin syiden ennaltaehkäisyyn sekä lasketaan RPN (1-1000). Jos riski ylittää sovitun luvun (esim. 100), on toimenpiteet mietittävä niin, että riski pienenee alle sovitun luvun. (Karjalainen, 2016) Yllä olevassa taulukossa 10 on esimerkki riskianalyysistä.

Alla on lueteltuna SFS-EN 31010 standardin mukaan FMEA/FMECA -analyysien käyttötarkoituksia:

- Auttamaan luotettavien suunnitteluvaihtoehtojen valinnassa
- Varmistamaan, että kaikki järjestelmien ja prosessien vikaantumismuodot sekä niiden vaikutukset onnistuneeseen toimintaan on otettu huomioon
- Tunnistamaan inhimillisiä virheitä ja niiden vaikutuksia
- Tarjoamaan perustan fyysisten järjestelmien testausten suunnittelulle ja kunnossapidolle
- Parantamaan menetelmien ja prosessien suunnittelua
- Tarjoamaan analyysitekniikoille, kuten vikapuuanalyysille, laadullisia ja määrällisiä tietoja

FMEA/FMECA analyysimenetelmän vahvuudet ja edut ovat:

- Välttää kalliiden laitemuutosten tarvetta käytön aikana, tunnistamalla ongelmat jo varhain suunnitteluprosessin aikana. (SFS-EN 60812:en, 2006) (SFS-EN 31010, 2013)
- Tunnistamaan viat, jotka yksin tai yhdessä ilmentyessään johtavat haitallisiin vaikutuksiin ja vaikuttavat toimintaan merkittävästi. (SFS-EN 60812:en, 2006)
- Määrittää vikamuodot, jotka voivat vaikuttaa toiminnallisuuteen. (Voi sisältää myös sekundäärisiä vikoja.) (SFS-EN 60812:en, 2006) Tunnistaa komponenttien vikaantumismuodot, niiden syyt ja vaikutukset järjestelmään, ja esittää ne helposti luettavissa olevassa muodossa (SFS-EN 31010, 2013).
- Määrittää tarpeen suunnittelumenetelmille, joilla parannetaan luotettavuutta esim. kahdennus, rasitukset, vikavarmuus, komponenttivalinnat yms. (SFS-EN 60812:en, 2006)
- Luo loogisen mallin, jolla voidaan arvioida vikojen tai poikkeavien toimintatilojen esiintymistiheyttä kriittisyysarviointia varten. (SFS-EN 60812:en, 2006)
- Paljastaa turvallisuusriskit ja todennäköiset ongelma-alueet tai epäyhteydenmukaisuudet viranomaisten määräysten kanssa. (SFS-EN 60812:en, 2006)
- Varmistaa, että testausohjelmalla voidaan paljastaa mahdollisia vioittumistapoja. (SFS-EN 60812:en, 2006)
- Keskittää tarkastelu avainalueisiin, joihin kannattaa kohdistaa laadunvalvontaa, tarkastustoimintaa ja valmistusprosessin valvontaa. (SFS-EN 60812:en, 2006)
- Auttaa ennakoivan kunnossapidon strategian ja aikataulutuksen luonnissa (SFS-EN 60812:en, 2006)
- Helpottaa tai tukee testauskriteereiden määrittämistä, testausohjelmia ja vianetsintäohjeita, esim. suorituskyky- ja luotettavuustestaus (SFS-EN 60812:en, 2006)

- Tukee käyttöön liittyviä toimenpiteitä, kuten vian seurausten ehkäisemisen suunnittelua ja erilaisten käyttötapojen suunnittelua. (SFS-EN 60812:en, 2006)
- Antaa suunnittelijoille ymmärrystä tekijöistä, jotka vaikuttavat järjestelmän luotettavuuteen (SFS-EN 60812:en, 2006)
- Tuottaa dokumentin, joka toimii todisteena, että on varmistettu huolella suunnitelman toimivuus palvelun määrityksien mukaisesti. Erittäin tärkeä tuotevastuussa. (SFS-EN 60812:en, 2006)
- Laajasti sovellettavissa inhimillisiin, järjestelmiä ja laitteita koskeviin vikaantumismuotoihin sekä laitteistoihin, ohjelmistoihin sekä menettelyihin. (SFS-EN 31010, 2013)
- FMEA-metodi edistää priorisoimaan vikamuotojen vaikutuksia (failure mode effects), jotta resurssit voidaan käyttää mahdollisimman tehokkaasti. (Trammell & Davis, 2001)
- Antaa panoksen valvontaohjelmien kehittämiseen korostamalla tärkeimpiä ominaisuuksia, joita pitää valvoa (SFS-EN 31010, 2013)

FMEA/FMECA analyysimenetelmän rajoituksia ja puutteita ovat mm:

- Niitä voi käyttää vain yksittäisten vikaantumismuotojen tunnistamiseen, ei vikaantumismuotojen yhdistelmiin (SFS-EN 31010, 2013). Suhteellisen heikko vikamuotojen tunnistus (Trammell & Davis, 2001). FMECA ei ota huomioon keskinäisiä riippuvuuksia erilaisten vikamuotojen ja vaikutusten keskuudessa. (Sachdeva;Kumar;& Kumar, 2009)
- Elleivät tutkimukset ole riittävästi keskitettyjä ja hallinnoituja, ne voivat olla kalliita ja aikaa vieviä ja vaatii eritaustaisia asiantuntijoita (SFS-EN 31010, 2013)
- FMEA on hyvin vaikea, väsyttävä ja työläs suorittaa monikerroksisille ja monimutkaisille järjestelmille, joilla on useita toimintoja ja jotka koostuvat useista komponenteista (SFS-EN 60812:en, 2006), (SFS-EN 31010, 2013). Menetelmä on erittäin raskas ja voi olla äärimmäisen haastava tiimin pitkäaikaiselle työn tehokkuudelle (Trammell & Davis, 2001).
- Inhimillisten virheiden ja huollon vaikutuksia ei tavallisesti sisällytetä analyysiin. (Ihmisen ja laitteiden vuorovaikutuksia käsitellään erikoismenetelmillä esim. tehtäväanalyysissä.) (SFS 5438, 1988)
- Vikoja tarkastellaan toisistaan riippumattomina: osittaisia ja samanaikaisia vikoja sekä yhteisvikoja vaikea määritellä. Huom! Inhimilliset ja ympäristötekijät muodostavat pääosan yhteisvikojen syistä. (SFS 5438, 1988)
- FMEA ei tarjoa systemaattista menetelmää järjestelmän poikkeamien arviointiin (muuta kuin jokaisen yksittäisen komponentin ja järjestelmän alikomponentin). (Trammell & Davis, 2001)
- Tietovarasto-ongelma: tarpeellinen tieto, jota käytetään FMEA:n tekoon, on vaikeasti saatavilla. (Daramola;Stålhane;& Moser, 2011)
- Tiedon prosessoimisen ongelma: aikaisemmat kokemukset ja tiedot ovat vaikeita hyödyntää. (Daramola;Stålhane;& Moser, 2011)

- Monimutkaisuuden ongelma: valtava ihmisten ajan ja resurssien tuhlaus. (Daramola;Stålhane;& Moser, 2011) → Ratkaisuna on, että vähennetään monimutkaisuutta pyrkimällä käyttämään yhtä tietokantaa. (Dittmann;Rademacher;& Zelewski, 2004)
- Integroinnin ongelma: on vaikea yhdistää asiantuntijuutta yrityksen eri näkökulmista laatuteknistä tietoa yhdistetyksi kokonaisuudeksi henkilökunnan kehittämistä varten. (Daramola;Stålhane;& Moser, 2011)
- Etsinnän ongelma: on vaikeaa tuottaa sopiva etsintäkriteeri FMEA tiedon kyselyyn. (Daramola;Stålhane;& Moser, 2011)
- Päivityksen ongelma: on vaikea pitää tietoa tietovarastoissa päivitettynä, erityisesti turhan työn välttämiseksi (Daramola;Stålhane;& Moser, 2011)
- Kolmenlaisia ominaisuuksia, kuten talous-, tuotantomäärä- ja turvallisuus näkökulma jne., joita ei ole otettu huomioon. (Sachdeva;Kumar;& Kumar, 2009)
- Oletetaan, että vakavuus (Severity), esiintyminen (Occurrence) ja havaitseminen (Detection) skaala indekseillä on sama mittari ja sama suunnittelutaso, joka vastaa samoja arvoja eri indeksiluokilla. Kolmen tekijöiden eri asetuksilla voidaan tuottaa täsmälleen sama RPN-arvo (Risk Priority Number), mutta piilovaikutus saattaa olla täysin erilainen. Kertomismenetelmä on kyseenalainen ja harhaanjohtava menetelmä (Sachdeva;Kumar;& Kumar, 2009) (SFS-EN 60812:en, 2006) (Bowles, 2003)

3.2.4 PSK 6800 Laitteiden kriittisyysluokittelu

PSK6800: 2008 Laitteiden kriittisyysluokittelu teollisuudessa standardi kuvaa VVKA:n menettelyn teollisuuden eri kohteiden kriittisyyden arvioinnin Tässä menettelyssä kriittisyyttä arvioidaan taloudellisten vaikutusten, henkilöturvallisuuden ja ympäristövaikutusten näkökulmista. Tätä menetelmää käytetään kunnossapitosuunnitelman lähtötiedon tuottamiseen. Lisäksi menetelmää voidaan käyttää esimerkiksi hankintavaiheen tukena määriteltäessä hankittavan kriittisen laitteen ominaisuuksia, laatutasoa ja vastaanottokriteerejä. Standardissa 6800 keskitytään kriittisyyden luokitteluun pääsääntöisesti taloudellisten vaikutusten perusteella. (PSK 6800, 2008)

PSK6800 standardin ero FMEA standardiin on painoarvokertoimet, jotka puuttuvat FMEA:sta. Painoarvokertoimet kuvaavat laitoksen prosessiteknisten toimintojen keskinäistä riippuvuutta. Painoarvokertoimia käytetään laitteen tuotannon menetyksen painoarvon Wp laskemiseen. Painoarvokertoimet ositetaan esimerkiksi prosessihierarkian mukaan siten, että koko laitoksen kannalta kriittinen laite saa painoarvon 100 %. Hierarkia voi olla esim. Laitos → tuotantoyksikkö → prosessi → osaprosessi. Tehtäessä PSK6800 mukaista VVKA:ta, siinä paneudutaan syvällisemmin laitteen kriittisyysindeksin K ja kriittisyyden osaindeksien (Ks, Ke, Kp, Kq ja Kr) laskentaan. Myöskään PSK6800 menetelmän taulukossa ei ole määritelty vian pois-

tamiseen suositeltuja toimenpiteitä, nimettyä vastuuhenkilöä ja aikataulua, mihin mennessä asia on hoidettava. Taulukosta puuttuu myös laitteen kriittisyyden uudelleenarviointi. Alla on taulukot 11 ja 12 vertailun vuoksi. Taulukossa 12 on ympyröity punaisella edellä mainitut toimenpiteet, jotka eivät PSK6800 luokitteluun sisälly.

Taulukko 11. Laitteiden kriittisyyden luokittelu teollisuudessa (PSK 6800, 2008)

PSK Standardisointi

LAITTEIDEN KRIITTISYYSLUOKITTELU TEOLLISUUDESSA
Criticality Classification of Equipment in Industry
2008-06-05

PSK 6800
Liite1

Laitos
Kriittisyysluokittelun kohde
Tekijät
Versio
Päiväys

Kriittisyyden raja-arvo 400
Tuotannon menetyksen painoarvokerroin Wp 100

Toimintopaikan tunniste	Toimintopaikan nimitys	Vikaantumisväli (1…8)	Turvallisuus (0…16)	Ympäristö 0…16	Tuotannon menetys (0…4)	Loppu-tuotteen laatukus-tannus (0…4)	Korjaus-kustannus (0…4)	Kriitti-syys-indeksi	Kriittisyyden osaindeksit				
		Painoarvot W -->	30	20	100	30	20	K	Ks	Ka	Kp	Kq	Kr
								0	0	0	0	0	0
								0	0	0	0	0	0
								0	0	0	0	0	0
								0	0	0	0	0	0
								0	0	0	0	0	0
								0	0	0	0	0	0
								0	0	0	0	0	0
								0	0	0	0	0	0
								0	0	0	0	0	0
								0	0	0	0	0	0
								0	0	0	0	0	0
								0	0	0	0	0	0
								0	0	0	0	0	0
								0	0	0	0	0	0
								0	0	0	0	0	0
								0	0	0	0	0	0
								0	0	0	0	0	0
								0	0	0	0	0	0
								0	0	0	0	0	0
								0	0	0	0	0	0
								0	0	0	0	0	0
								0	0	0	0	0	0

Taulukko 12. Esimerkki prosessi-FMEA taulukosta (Weibull, 2015)

POTENTIAL
FAILURE MODE AND EFFECTS ANALYSIS
Front Door L.H.

FMEA Type
Item 1.1.1 - Front Door L.H.
Model Year(s)/Vehicle(s) 20XX/Lion 4dr/Wagon
Core Team A. Tate Body Engrg, J. Smith - OC, R. James - Production, J. Jones - Maintenance

Process Responsibility Body Engineering
Key Date 3/10/2015

FMEA Number 1450
Page 1 of 1
Prepared By J. Ford - X6521 - Assy Ops
FMEA Date (Orig.) 3/10/2015 (Rev) 3/21/2015

Name / Function / Requirements	Potential Failure Mode	Potential Effect(s) of Failure	SEVi	Classification	Potential Cause(s) of Failure	OCCi	Current Process Controls (Prevention)	Current Process Controls (Detection)	DETi	RPNi	Recommended Action(s)	Responsibility & Planned Completion Date	Action Results: Actions Taken & Actual Completion Date	SEVr	OCCr	DETr	RPNr
1.1.1 - Front Door L.H.																	
Op. 70 Manual application of wax inside door/ cover inner door, lower surfaces with wax to specification thickness.	Insufficient wax coverage over specified surface	Allows integrity breach of inner door panel. Corroded interior lower door panels. Deteriorated life of door leading to: - Unsatisfactory appearance due to rust through paint over time - Impaired function of interior door hardware	7		Manually inserted spray head not inserted far enough	8		Visual check each hour - 1/shift for film thickness (depth meter) and coverage.	5	280	Add positive depth stop to sprayer.	Mfg Engrg - 3/10/2003	Stop added, sprayer checked on line.	7	2	5	70
											Automate spraying.	Mfg Engrg - 3/10/2003	Rejected due to complexity of different doors on same line.				
					Spray head clogged- Viscosity too high- Temperature too low- Pressure too low.	5	Test spray pattern at start-up and after idle periods, and preventive maintenance program to clean heads.	Visual check each hour - 1/shift for film thickness (depth meter) and coverage.	5	175	Use Design of Experiments (DOE) on viscosity vs. temperature vs. pressure.	Mfg Engrg - 3/10/2003	Temp and press limits were determined and limit controls have been installed - control charts show process is in control Cpk = 1.85.		1	5	35
					Spray head deformed due to	2	Preventive maintenance	Visual check each hour - 1/shift for	5	70					2	5	70

PSK 6800 standardin mukaan kriittisyyden arviointi tehdään seuraavasti:

- Määritetään tarkastelun laajuus
- Määritetään standardin kohdan 5 mukaan tuotannon menetyksen painoarvo WP.
- Arvioidaan sopivatko standardin taulukossa 1 annetut muut painoarvot sovellettavalle teollisuuden toimialalle. Tarvittaessa standardissa annettuja painoarvoja muutetaan.

1. Listataan standardin liitteenä 1 olevaan taulukkolaskentaohjelmaan tarkasteltavat laitteet
2. Valitaan tarkasteltaville laitteille standardin taulukosta 1 käytettävät kertoimet.
3. Ohjelma laskee laitteiden kriittisyysindeksin (K) ja sen osaindeksit (K_s, K_e, Kp, Kq ja K_r) käyttäen hyväksi annettuja parametreja.
4. Kriittisyysluokittelu tehdään lajittelemalla laitteet kriittisyysindeksin K mukaiseen järjestykseen

Mikäli laitteiden kriittisyyttä halutaan tarkastella vain esimerkiksi laatukustannusten kannalta, käytetään lajitteluperusteena kriittisyyden osaindeksiä K_q.

Mikäli riski kohdistuu turvallisuuteen tai ympäristöön, on sen suuruuden selvittämiseksi käytettävä yleisesti hyväksyttyjä riskianalyysimenettelyjä ja niistä saatavien tulosten avulla pienennettävä riski viranomaisten vaatimalle tasolle. Tämä menetelmä ei ota kantaa työturvallisuuteen. Sitä varten on olemassa omat ohjeet ja säädökset. (PSK 6800, 2008)

3.3 POIKKEAMATARKASTELU HAZOP

Poikkeamatarkastelu (HAZOP), joka tulee englanninkielen sanoista Hazard and Operability study. Lisäksi käytetään termiä Hazard and Operability analysis. HAZOP on vaarojen tunnistamisen perusmenetelmä, joka arvioi systemaattisesti järjestelmän kunkin osan sekä tutkii miten poikkeamat suunnittelutavoitteista voivat sattua ja voivatko ne aiheuttaa ongelmia. (SFS-EN 61882:en, 2016), (SFS-IEC 60300-3-9, 2000) HAZOP-prosessi on laadullinen tekniikka. Se perustuu ohjaaviin kysymyksiin, miksi käyttötarkoitusta tai toimintaehtoja ei saavuteta suunnittelun, prosessin, menetelmän tai järjestelmän jokaisessa vaiheessa. Tämän prosessin suorittaa yleensä monitieteellinen ryhmä kokoussarjan aikana. (SFS-EN 31010, 2013)

Standardin SFS-EN 31010 mukaan HAZOP on lähes samanlainen kuin FMEA, koska sillä tunnistetaan prosessin, järjestelmän tai menetelmän vikaantumismuodot ja niiden syyt sekä seuraukset. Erona on se, että ryhmä miettii haitallisia tuloksia ja poikkeamia aiotuista tuloksista ja tilanteista. Menetelmä palaa seuraavaksi takaisin mahdollisiin syihin ja vikaantumismuotoihin, kun taas FMEA aloittaa vikaantumismuotojen tunnistuksella. (SFS-EN 31010, 2013) Myös standardin SFS-IEC 60300-3-9 mukaan HAZOP on eräs vika- ja vaikutusanalyysin (VVA) muoto.

HAZOP on alun perin kehitetty kemian teollisuuteen. Se on järjestelmällinen tekniikka toimintaongelmien ja vaarojen tunnistamiseen koko laitteistossa. Se on erittäin käyttökelpoinen tunnistamaan ennalta tuntemattomia vaaroja, joita on jäänyt suunniteltuun laitteistoon puutteellisen tiedon vuoksi, tai joita on syntynyt olemassa olevaan laitteistoon prosessiolosuhteiden tai käyttötapojen muutosten vuoksi. (SFS-IEC 60300-3-9, 2000) Poikkeamatarkastelun perustavoitteet ovat.

a. tuottaa laitteiston tai prosessin täydellinen kuvaus sisältäen suunnitteluperusteet,
b. tarkastella järjestelmällisesti prosessin tai laitteiston jokainen osa, jotta paljastetaan, miten poikkeamat suunnitteluperusteista voivat sattua, ja
c. päättää, voivatko nämä poikkeamat johtaa toimintaongelmiin tai vaaroihin.

HAZOP-prosessi voi käsitellä kaiken muotoisia poikkeamia suunnitellusta tarkoituksesta. Poikkeamat voivat johtua puutteellisesta suunnittelusta, yhdestä tai useammasta komponentista, suunnitelluista menetelmistä tai ihmisten toiminnoista. HAZOP-tutkimusta käytetään tavallisesti yksityiskohtaisen suunnittelun vaiheessa. Tällöin on saatavilla aiotun prosessin täydellinen kaavio, mutta suunnittelumuutokset ovat vielä käytännössä mahdollisia. Kun käytetään vaiheittaista lähestymistapaa, sitä voidaan soveltaa erilaisia viitesanoja käyttäen, jolloin annetaan ohjeita yksityiskohtaisen suunnittelun edistyessä jokaisessa vaiheessa. Tutkimusta voidaan suorittaa myös käytön aikana, mutta tällöin tarvittavat muutokset voivat olla kalliita. (SFS-EN 31010, 2013)

Tämän poikkeamatarkastelun periaatteita voidaan soveltaa käynnissäoleviin tai suunnittelun eri vaiheessa oleviin prosessilaitoksiin. Suunnittelun aikaisessa vaiheessa tehty poikkeamatarkastelu voi usein tuottaa ohjeita turvallisempaan yksityiskohtien suunnitteluun. Yleensä poikkeamatarkastelu tehdään yksityiskohtaisen suunnittelun vaiheessa ja sitä kutsutaan ”HAZOP II”:ksi. Alla oleva taulukko on esimerkki HAZOP II lomakkeesta. (SFS-IEC 60300-3-9, 2000)

Taulukko 13. Esimerkki poikkeamatarkastelun lomakkeesta (SFS-IEC 60300-3-9, 2000)

Avainsana	Poikkeama	Mahdolliset syyt	Seuraukset	Tarvittava toimenpide
Ei, ei mitään	Ei virtausta	1) Syötettävää materiaalia ei käytettävissä	Tuotetun aineen määrä vähenee. Muodostuu polymeeriä	a) Varmista hyvä kommunikaatio operaattorin kanssa b) Alarajahälytys annostelusäiliöön
		2) Pumppu vioittuu (erilaisista syistä)	Kuten kohdassa1)	Kuten kohdassa b)
		3) Tukos tai venttiili suljettu erehdyksessä tai ohjausventtiili vioittuu kiinni	Kuten kohdassa A.1 Pumppu ylikuumenee	Asennetaan kullekin pumpulle takaisinkiertopiiri

Alla on lueteltuna HAZOPin hyviä puolia:

- Monimutkaiset järjestelmät jaetaan pienemmiksi paremmin johdettavimmiksi ”nodeiksi” eli solmupisteiksi (Trammell & Davis, 2001).
- Sen avulla tunnistetaan järjestelmällisesti prosessiparametrien hajonta, jolloin järjestelmän vikaantumismuotojen tunnistaminen tulee mahdolliseksi (Trammell & Davis, 2001).
- Se huomioi selkeästi inhimillisten virheiden syyt ja seuraukset (SFS-EN 31010, 2013)
- Tunnistaa vaarat ja tapahtumat, jotka johtavat onnettomuuteen, päästöön tai muuhun ei-toivottuun tapahtumaan. (SFS-EN 61882:en, 2016)
- Se antaa keinot tutkia systemaattisesti järjestelmät, prosessit tai menetelmät (SFS-EN 31010, 2013).
- Se soveltuu monille järjestelmille, prosesseille ja menetelmille (SFS-EN 31010, 2013).
- Siihen liittyy monitieteellinen ryhmä, jolla on tosielämän käyttökokemusta ja mahdollisesti mukana niitä, jotka vastaavat käsittelytoimenpiteistä (SFS-EN 31010, 2013).
- Se tuottaa ratkaisuja ja riskinkäsittelytoimenpiteitä (SFS-EN 31010, 2013).
- Se tallentaa prosessin kirjallisesti, mitä voidaan käyttää oikeanlaisen huolellisuuden osoittamiseen. (SFS-EN 31010, 2013).

Ja seuraavana on lueteltuna HAZOPin huonoja puolia:

- Ei ole vahva tai tarpeeksi tehokas vikavaikutusten priorisoinnissa. (Trammell & Davis, 2001).
- HAZOP ei tavallisesti ota selvää korjaavien toimintojen suhteellisia vaikutuksia. (Trammell & Davis, 2001)
- Ei ole vahva analysoimaan tunnistettujen korjaavien toimenpiteiden suhteellisia vaikutuksia (Rong;Zhao;& Yu, 2008).
- Vaatii merkittävää resurssien sitoutumista (SFS-EN 61882:en, 2016).
- Prosessi on yksitoikkoinen ja osallistujien mielenkiinnon ylläpitäminen voi olla haasteellista (SFS-EN 61882:en, 2016).
- Koska mentelmä on laadullinen, tuloksia ei siten voida määrällisesti arvioida (Guo & Kang, 2015).
- Yksityiskohtainen analyysi voi olla erittäin aikaa vievää ja sen tähden kallista (SFS-EN 31010, 2013).
- Yksityiskohtainen analyysi vaatii korkeatasoisen dokumentoinnin tai järjestelmän/prosessin ja menetelmän määrittämisen (SFS-EN 31010, 2013).
- Se voi keskittyä löytämään yksityiskohtaisia ratkaisuja mieluummin kuin haastamaan perusoletuksia (tätä voidaan lieventää käyttämällä vaiheittaista lähestymistapaa) (SFS-EN 31010, 2013).

- Keskustelu voi keskittyä suunnitelman yksityiskohtiin, mutta ei laajempiin ja ulkoisiin asioihin (SFS-EN 31010, 2013).
- Sitä rajoittavat suunnitelma (luonnos) ja suunniteltu tarkoitus sekä ryhmälle annetun tehtävän laajuus ja tavoitteet (SFS-EN 31010, 2013).
- Prosessi perustuu pitkälti suunnittelijoiden asiantuntemukseen. Voi olla vaikeaa olla riittävän objektiivinen etsiessään ongelmia omista suunnitelmistaan (SFS-EN 31010, 2013).

HAZOPia vastaavanlainen menetelmä on elintarvike- ja lääkevalmistusteollisuudessa käytettävä HACCP - Hazard analysis and critical control point, operatiivisten riskien vaikutusten arviointia tukeva riskiarviointimenetelmä. HACCP on systemaattinen, ennakoiva ja ehkäisevä järjestelmä varmistamaan tuotteen laatu, prosessien toimintavarmuus ja turvallisuus mittaamalla ja valvomalla ominaisuuksia, joiden tulee olla määrätyissä rajoissa. HACCP alkaa perusvuokaaviosta tai prosessikaaviosta ja tiedoista niistä vaaroista, jotka voivat vaikuttaa prosessin tuotoksen tai tuotteen laatuun, turvallisuuteen tai toimintavarmuuteen. HACCP-menetelmän panos on tiedot vaaroista ja niiden riskeistä sekä keinot, joilla niitä voidaan valvoa. (SFS-EN 31010, 2013)

Standardin SFS-EN 31010 mukaan HACCP-menetelmä koostuu seuraavista seitsemästä periaatteesta:

- tunnistaa vaarat ja ehkäisevät toimenpiteet, jotka liittyvät näihin vaaroihin
- määrittää prosessin kohdat, joissa vaaroja voi valvoa tai poistaa (the Critical Control Points eli CCPt)
- määrittää kriittiset raja-arvot, joita tarvitaan vaarojen seuraamisessa eli jokaisen kriittisen seurantapisteen (CCP) tulisi toimia määritettyjen parametrien sisällä sen varmistamiseksi, että vaarat ovat valvonnassa
- seurata määritellyin väliajoin kriittisiä rajoja jokaisessa CCP:ssä
- laatia korjaavat toimenpiteet, jos prosessi ylittää sille asetetut rajat
- laatia todentamismenetelmät
- toteuttaa jokaiselle vaiheelle kirjanpito- ja dokumentointimenetelmä. (SFS-EN 31010, 2013)

3.4 JUURISYYANALYYSI (RCA)

Root cause analysis eli RCA on vaaratapahtuman tutkintamenetelmä. Sillä pyritään tunnistamaan tapahtumien taustalla olevat organisaation toiminnassa piilevät riskit ja puutteet turvallisuuden varmistamisessa. Tämän analyysin tavoite on ymmärtää riittävän syvällisesti tapahtuman aiheuttanut tekijä. Analysointimenetelmä on julkaistu Max Ammermanin vuonna 1998 julkaistussa teoksessa The Root Cause Analysis Handbook: A Simplified Approach to Identifying, Correcting and Reporting Workplace Errors. (Terveyden ja hyvinvoinnin laitos, 2015)

Juurisyiden analyysi (RCA) on keskittynyt arvioimaan vahinkoja, jotka johtuvat erilaisista vikaantumistyypeistä. Tarkoituksena tunnistaa taustalla olevat tai alkuperäiset syyt sen sijaan, että käsittelisi vain välittömästi selviä oireita. Tiedetään, että korjaava toimenpide ei aina ole täysin tehokas ja että jatkuva parantaminen voi olla tarpeen (SFS-EN 31010, 2013). Merkittävä ero on, että RCA:n avulla tarkastelu painottuu sattuneeseen tapahtumaan ja siten analysoi mennyttä. Kuitenkin tieto jo tapahtuneista perussyistä voivat johtaa toimiin, jotka tuottavat parannuksia tulevaisuudessa. (SFS-EN 62740:en, 2015)

Juurisyyanalyysi standardi SFS-EN 62740 Root Cause Analysis, on yleinen standardi ja ei nimenomaisesti ole osoitettu turvallisuuden tai onnettomuuden tutkimista varten, vaikka standardissa kuvattuja menetelmiä voidaan käyttää em. tarkoitukseen. (SFS-EN 62740:en, 2015) Turvallisuuspohjaista juurisyiden analyysiä käytetään onnettomuustutkintaan ja työturvallisuuteen.

Asiantuntijaryhmä tekee juurisyyanalyysin. Alla on lueteltuna analyysin käyttöalueita:

- vikaantumisanalyysiä käytetään teknologisissa järjestelmissä liittyen toimintavarmuuteen ja kunnossapitoon
- tuotantopohjaista juurisyiden analyysiä käytetään laadunvalvonnan alueella teollisessa valmistuksessa
- prosessipohjainen juurisyiden analyysi keskittyy liiketoimintaprosesseihin
- Järjestelmäpohjainen juurisyiden analyysi on kehitetty edellisten alueiden yhdistelmänä, ja se käsittelee monimutkaisia järjestelmiä muutostenhallinnan, riskienhallinnan ja järjestelmäanalyysin kanssa. (SFS-EN 31010, 2013)
- Järjestelmällinen analyysitekniikka voi koostua yhdestä seuraavista kohdista:
- ”minkä vuoksi” kysytään 5 kertaa toistaen, eli 5 x Miksi? -menetelmä. Tällä pyritään kuorimaan syitä ja alisyitä kerros kerrokselta
- vika- ja vaikutusanalyysi (FMEA)
- vikapuuanalyysi (FTA)
- kalanruoto- tai Ishikawa-kaaviot (syy ja seuraus analyysi)
- Pareto-analyysi
- juurisyiden kartoitus. (SFS-EN 31010, 2013)

Standardin SFS-EN 31010 mukaan juurisyiden analyysin vahvuuksiin sisältyy seuraavat:

- sopivien asiantuntijoiden mukanaolo työryhmässä
- järjestelmällinen analyysi
- kaikkien todennäköisten oletusten tarkastelu
- tulosten dokumentointi
- tarve tuottaa lopulliset suositukset (SFS-EN 31010, 2013)

Standardin SFS-EN 31010 mukaan juurisyiden analyysin rajoitukset ovat seuraavat:

- Tarvittavia asiantuntijoita ei välttämättä ole käytettävissä.
- Kriittinen näyttö voi tuhoutua vikaantumistilanteessa tai se voidaan puhdistuksen aikana hävittää.
- Ryhmällä ei ole tarpeeksi aikaa tai resursseja täysin arvioida tilannetta.
- Mahdollisesti suosituksia ei voida riittävästi ottaa käyttöön. (SFS-EN 31010, 2013)

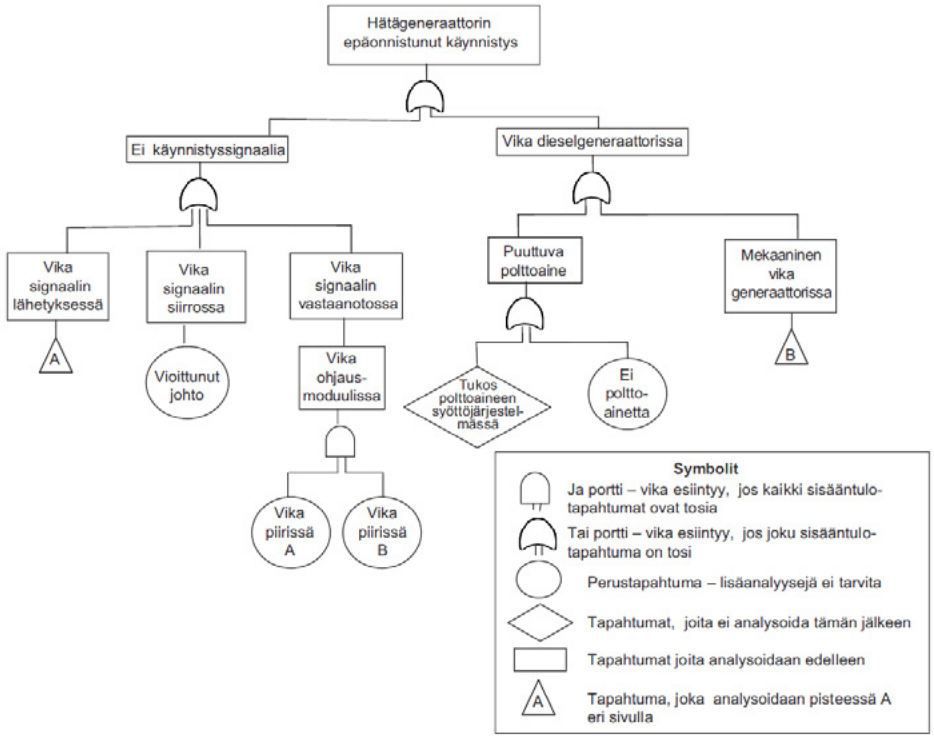
Juurisyyanalyysi on tehokas työkalu tutkimaan asioita, jotka ovat vaikuttaneet ihmisten tai järjestelmien toimintaan organisaatiossa. Juurisyyanalyysi voidaan määritellä seuraavasti: Mitä tahansa rakennettua prosessia käytetään ymmärtämään menneisyyden tapahtumien aiheuttajaa, jonka tarkoituksena on estää tapahtumien toistuminen. (Wilbur, 2016)

4 Täydentävät menetelmät

Yleisimmille riskianalyysimentelmille löytyy useita täydentäviä menetelmiä, mutta tässä selvityksessä on otettu tarkasteluun vikapuuanalyysi (FTA) ja ihmisen luotettavuuden arviointi (HRA) menetelmät.

4.1 VIKAPUUANALYYSI (FTA)

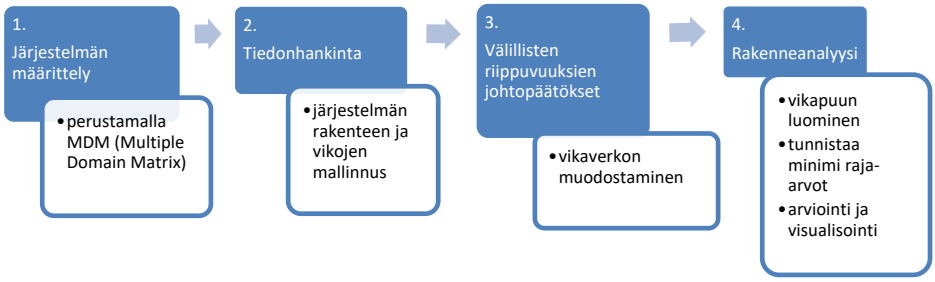
Vikapuuanalyysillä (engl. Fault tree analysis, FTA.) esitetään järjestelmän vikaantumista kuvaavaa rakennetta graafisesti. Se koostuu vikaantumista kuvaavista tapahtumista. Epätoivottu tapahtuma asetetaan puurakenteessa ylimmäksi ja tästä käytetään nimitystä huipputapahtuma (TOP event). Tekijät, jotka vaikuttavat huipputapahtumaan, ovat tyypillisesti komponenttien vikaantumisia ja ihmisten virheitä, mutta menetelmä mahdollistaa monipuolisesti myös muiden huipputapahtumaan vaikuttavien tekijöiden huomioimisen. (SFS-EN 61025:en, 2007). Kuvassa 13 on esimerkki vikapuuanalyysistä.



Kuva 13. Esimerkki standardin IEC 60300-3-9 mukaisesta vikapuuanalyysistä (SFS-EN 31010, 2013)

Vikapuu käsikirjan (Fault Tree Handbook) kirjoittajat (Vesely;Goldberg;Roberts;& Haasl, 1981) ovat tarkastelleet induktiivisia menetelmiä kahdesta syystä. Ensimmäiseksi, induktiiviset tekniikat ovat hyödyllisiä ja valaisevia verrattuna pelkkään vikapuuanalyysiin. Toiseksi, niille järjestelmille, joille ei ole vikapuuanalyysiin varattu kustannuksia tai parannuksia, induktiiviset metodit antavat pätevän ja systemaattisen keinon tunnistaa ja korjata ei-toivottuja ja vaarallisia olosuhteita. Tästä syystä vikapuuanalyytikon olisi tärkeää ymmärtää syvällisesti nämä vaihtoehtoiset käytänteet.

Vikapuuanalyysit kuuluvat turvallisuusanalyysimenetelmiin ja ne vaativat valtavasti manuaalista työtä ja asiantuntemusta. Kirjoittamassaan artikkelissa (Roth;Wolf;& Lindemann, 2015) ovat sitä mieltä, että tehokkuutta edellämainittuihin analyyseihin on parannettava. He ovat kehitelleet räätälöidyn lähestymistavan, jolla generoidaan ja arvioidaan vikapuita käyttämällä matriisiin perustuvia malleja. Tämä menetelmä on tarkoitettu käytettäväksi järjestelmän- tai laitesuunnittelun varhaisessa vaiheessa. Automaattisesti luodut vikapuut helpottavat tunnistamaan turvallisuuskriittisiä osia, vertaillen ja arvioiden vaihtoehtoisia käsitteitä. Kehitetty lähestymistapa käsittää neljä vaihetta ja kuusi askelta (toimenpidettä), jotka ovat kuvan 14 mukaiset.



Kuva 14. Menettely, jolla generoidaan ja arvioidaan (lasketaan) vikapuita (Roth;Wolf;& Lindemann, 2015)

4.2 IHMISTEN LUOTETTAVUUDEN ARVIOINTI (HRA)

Ihmisen luotettavuuden arviointi, Human Reliability Assessment (HRA), käsittelee ihmisten vaikutuksia järjestelmän toimintakyvylle ja HRA-analyyseja voidaan käyttää arvioitaessa inhimillisten virheiden vaikutustapoja järjestelmään. Analyysin avulla voidaan tuoda esille virheitä, jotka voivat haitata tuottavuutta ja paljastamaan, miten käyttö- ja kunnossapitohenkilöstö voi ”korjata” nämä virheet ja muut viat esim. laitteistosta ja ohjelmistosta. (SFS-EN 62508:en, 2011)

HRA-analyysi tehdään joko määrällisen tai laadullisen tutkimuksen avulla. Laadullisen analyysin avulla tunnistetaan mahdolliset inhimilliset virheet ja niiden syyt, jotta virheen todennäköisyyttä voidaan pienentää. Määrällinen analyysi tuottaa tietoja esim. vikapuuanalyysille ja muille tekniikoille (SFS-EN 62508:en, 2011). Bell ja Holroyd kävivät läpi HRA-tekniikoiden valikoimaa ja arvioivat niiden heikkokuksia ja vahvuuksia tutkimusraportissaan ”Review of human reliability assessment methods”. He löysivät ihmisen luotettavuuteen liittyvää työkalua ja lyhennettä yhteensä 72 kappaletta, joista 35 kappaletta tutkittiin tarkemmin. Viimeksi mainituista valikoitui siten 17 HRA:han liittyvää työkalua, joiden katsottiin olevan käyttökelpoisia arvioitaessa teollisuudessa terveys-, turvallisuus- ja ympäristöasioita ja siten mahdollisesti käytettäväksi HSE (health safety and environment) asioista päättäville henkilöille. (Bell & Holroyd , 2009)

Tutkimuksessa (Aalipour;Ayele;& Barabadi, 2016) kerrotaan, että ihmisen luotettavuus vaikuttaa merkittävästi kaikkien tuotantoprosessien huoltotöihin, turvallisuuteen ja kustannustehokkuuteen. Ihmisten luotettavuuden parantamiseksi ihmisvirheiden syyt olisi tunnistettava ja ihmisten virheiden todennäköisyys olisi määritettävä. Ihmisvirheen analyysi on hyvin tapauskohtainen ja alan konteksti olisi otettava huomioon. Heidän tutkimuksensa tavoitteena oli tunnistaa ihmisten virheiden syyt ja parantaa ihmisten luotettavuutta kaapeliteollisuudessa. Tutkimusraportin keskeisena painopisteenä he käyttivät kolmea yleisintä HRA-tekniikkaa, jotka olivat:

- HEART (Human Error Assessment and Reduction Technique) eli inhimillisten virheiden arviointi- ja vähentämistekniikka,
- SPAR-H (Standardized Plant Analysis Risk - Human Reliability), standardisoitu laitos/tehdas analyysi riskeille, mukana ihmisen luotettavuus
- BN (Bayesian Network) - ihmisen virheen todennäköisyyden arvioimiseksi ja tarkistettujen tulosten johdonmukaisuuden tarkastamiseksi.

Tapaustutkimusten tulokset osoittivat, että inhimillisen erehdyksen tärkeimmät syyt huoltotoimien aikana ovat ajankohta, kokemuksen puute ja heikot ohjeet. Käyttämällä em. kolmea tekniikkaa, saatiin lähes samanlaiset todennäköisyydet ihmisten aiheuttamille virheille. (Aalipour;Ayele;& Barabadi, 2016)

Standardin (SFS-EN 31010, 2013) mukaan HRA-prosessi on seuraavanlainen:

- Ongelman määrittely; minkä tyyppiset ihmisen osallistumiset olisi tutkittava/arvioitava?
- Tehtävän analysointi; miten tehtävä suoritetaan ja millaisia apuvälineitä tarvitaan suoritusta tukemaan?
- Inhimillisen virheiden analysointi; kuinka tehtävän voi tehdä väärin, mitä virheitä voi tapahtua ja miten ne voidaan korjata?
- Kuvaus; miten nämä virheet ja väärin tekemiset voidaan sisällyttää muihin laitteisto-, ohjelmisto- ja ympäristötapahtumiin, jotta saataisiin kaikenkattava järjestelmän vikaantumistodennäköisyys laskettua?
- Seulonta, onko mitään virheitä tai tehtäviä, jotka eivät vaadi yksityiskohtaista määritystä?
- Määrittäminen; kuinka todennäköisiä yksittäiset virheet ja tehtävien epäonnistumiset ovat?
- Vaikutuksen arviointi; mitkä virheet tai tehtävät ovat tärkeimpiä eli ne, joilla on suurin vaikutus luotettavuuteen tai riskiin?
- Virheiden vähentäminen; kuinka voidaan saavuttaa parempi ihmisen toimintavarmuus?
- Dokumentointi; mitä yksityiskohtia HRA-analyysistä on dokumentoitava? (SFS-EN 31010, 2013)

5 Muiden menetelmien yhdistelmämenetelmät

Aiemmin tässä raportissa on käyty läpi mitä mm. VVA, FMEA, VVKA, HAZOP, RCA tarkoittavat ja mitä riskianalyysit ovat yleisellä tasolla. Lisäksi tässä julkaisussa on esitetty edellä mainittujen menetelmien parhaita puolia ja epäkohtia. Yhdistämällä näitä eri analyysejä pyritään hyödyntämään kaikkien menetelmien parhaat puolet ja löytämään niistä käyttökelpoisimmat osa-alueet TPA menetelmän luomiseen. Tässä kirjallisuusselvityksessä on selvitetty ennen varsinaisen TPA-menetelmän kehittämistä varten olemassa olevia menetelmiä, joita on jo yhdistetty. Menetelmän kehittämistä varten haluttiin tietää, löytyykö menetelmiä, joissa otetaan huomioon sekä tuotannon kokonaistehokkuus, että turvallisuus- ja ympäristöriskit. Tarkastelun kohteena ovat myös eri analyysimenetelmien samankaltaiset elementit, jolloin nämä päällekkäisyydet joudutaan käsittelemään useaan kertaan eri menetelmiä käytettäessä.

5.1 TPA MENETELMÄÄ TUKEVA ESISELVITYS

Tuleva TPA menetelmä on yhdistelmä useita eri riskianalyysimenetelmiä, kuten FMEA, FMECA, HAZOP ja RCA. Eri menetelmillä on tarkoitus hallita sekä menneitä että tulevia riskejä, vikasyitä ja seurauksia (Mollah;Baseman;& Long, 2013). Kirjassa ”Risk Management Applications in Pharmaceutical and Biopharmaceutical Manufacturing” (Mollah;Baseman;& Long, 2013) tekijät toteavat, että mikäli seurauksia ei kyetä estämään ne pyritään ainakin minimoimaan. Tämä on yksi osatekijä, joka vahvistaa toiminta-ajatusta TPA menetelmän kehittämisessä. Mikään riskianalyysitekniikka yksinään ei ole riittävä hallitsemaan riskejä (Frosdick, 1997).

Riskinarviointi voidaan luokitella induktiiviseen ja deduktiiviseen riskinarviointiin tai molempiin (Mollah;Baseman;& Long, 2013). Induktiiviset menetelmät, kuten FMEA, FMECA ja HAZOP tarkastelevat tulevaisuuden tapahtumia ja ennustavat riskejä ja soveltuvat määrittelemään mitkä (vika)tilat ovat mahdollisia. Tapahtumien ja riskien estämiseksi on suunniteltava toimenpiteet. Esimerkiksi vikapuuanalyysi (FTA) on deduktiivinen menetelmä, joka katsoo ajassa taaksepäin ja selvittää kuinka usein (vika)tila voi esiintyä. (Vesely;Goldberg;Roberts;& Haasl, 1981)

Yleisin tilanne, jossa suoritetaan sekä induktiivinen että deduktiivinen riskinarviointi, on tapahtuma, jossa on tarvetta selvittää mikä meni pieleen eli tarkastella takautuvasti. Täyttä arviointia tarvitaan tilanteissa, missä pitää arvioida mitä muuta voi mennä pieleen. (Mollah;Baseman;& Long, 2013). Induktiivinen analyysi suoritetaan ensin ja sen jälkeen suoritetaan deduktiivinen analyysi (Lee & McCormick, 2012).

Taulukossa 14 on esitetty erilaisia riskinarviointityökaluja ja verrattu niitä toisiinsa pohjautuen:

- Laajuuteen (scope) – toteutettavan riskianalyysin laajuus
- Kuinka moneen osaan jako (granularity) – millä tarkkuudella analyysi suoritetaan ja dokumentoidaan
- Induktivinen vai deduktiivinen – induktiivinen on eteenpäin katsovaa ja suunniteltu, kun taas deduktiivinen on ajassa taaksepäin katsova.
- Vuorovaikutteinen versus yksittäinen riski.
- Monimutkaisuus (complexity) – monimutkaisuuden aste alhaisesta korkeaan.

Taulukko 14. Riskinarviointi työkalujen vertailua (Mollah;Baseman;& Long, 2013)

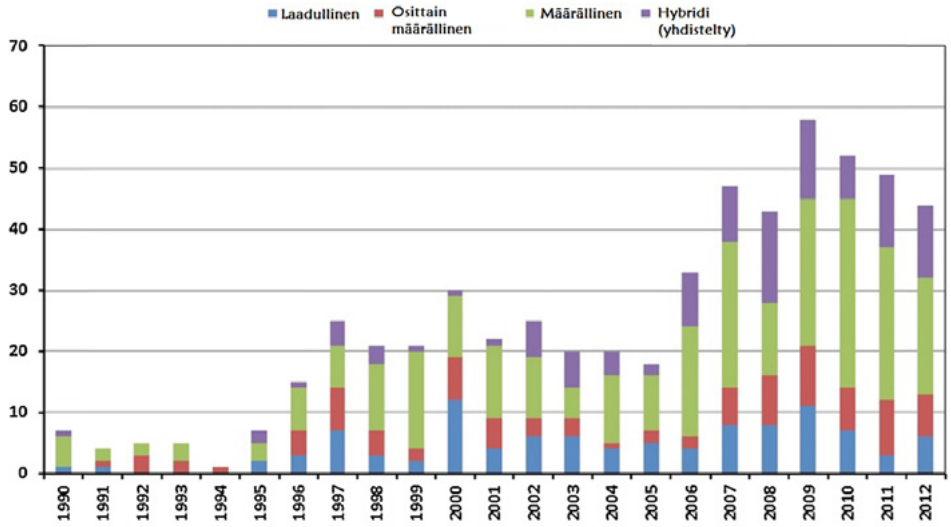
Risk Assessment Tool	Scope	Granularity	Inductive/ Deductive	Interactions vs. Individual Risks	Complexity
PHA	Any	Low	Either	Individual	Low
HAZOP	Focused	High	Inductive	Individual	Medium
HACCP	Any	Variable	Either	Individual	Low
FMEA	Any	High	Inductive	Individual	Medium
FTA	Focused	High	Deductive	Interactions	High
RRF	Broad	Low	Inductive	Individual	Low

Yllä olevassa taulukossa 14 verrataan PHA, HAZOP, HACCP, FMEA, FTA, ja RRF (Risk Ranking and Filtering) -analyysejä. Esimerkiksi riskinarviointityökaluista HACCP:n osiin jakautuneisuus riippuu siitä, mikä työkalu on valittu riskinarviointiin. HACCP ei määrittele käytettävää riskianalyysimentelmää, joten siinä voidaan käyttää joko induktiivista tai deduktiivista tekniikkaa.

Tutkimuksessaan ”Methods and models in process safety andrisk management: Past, present and future” (Khan;Rathnayaka;& Ahmed, 2015) tarkastelivat eri menetelmien ja mallien kehittymistä prosessien turvallisuuden ja riskinhallinnan osalta. Tarkastelu pohjautui lähes 600 artikkeliin, jotka oli julkaistu turvallisuus-, riski- ja luotettavuusalan johtavissa aikakausilehdissä sekä avoimessa kirjalliuudessa.

Alla olevasssa kuvassa 15, on tutkimuksen pohjalta havainnollistettu eri analyysimenetelmien/tekniikoiden jakautuminen kahden viimeisen vuosikymmenen ajalta. Eri analyysimentelmät voidaan jakaa laadullisiin; osittain määrällisiin, määrällisiin ja hybridi eli yhdistettyihin analyysimenetelmiin. Kuviosta voidaan havaita määrällisten (vihreällä merkitty) ja yhdistelmä (hybridi) menetelmien tutkimusten kasva-

neen enemmän kuin laadullisten tai puolittain määrällisten menetelmien käytön tutkimus. Tämä merkitsee sitä, että edellä mainittujen menetelmien käyttö on mielekästä prosessiturvallisuutta määriteltäessa ja riskienhallinnissa. (Khan;Rathnayaka;& Ahmed, 2015, s. 120)



Kuva 15. Analyysimenetelmien jakautuminen kahden viimeisen vuosikymmenen ajalta (Khan;Rathnayaka;& Ahmed, 2015)

Laadulliset menetelmät ovat ei-numeerisia menetelmiä, joita edustaa mm. HAZOP. Määrälliset menetelmät antavat realistisen numeerisen arvion, jotta saataisiin parempi ymmärrys ja tieto päätöksentekoa varten. (Khan;Rathnayaka;& Ahmed, 2015, ss. 120-127)

Hybridi menetelmät ovat yhdistelmä sekä laadullisista että määrällisistä analyysimenetelmistä. Menetelmä eroaa osittain määrällisestä, koska se tarjoaa tarkemman ja realistisemman määrällisen tuloksen. Hybridimenetelmiä on kehitetty mm. vaarojen tunnistamiseen ja analysointiin, riskien arviointiin sekä turvallisuuden hallintaan. (Khan;Rathnayaka;& Ahmed, 2015, s. 132)

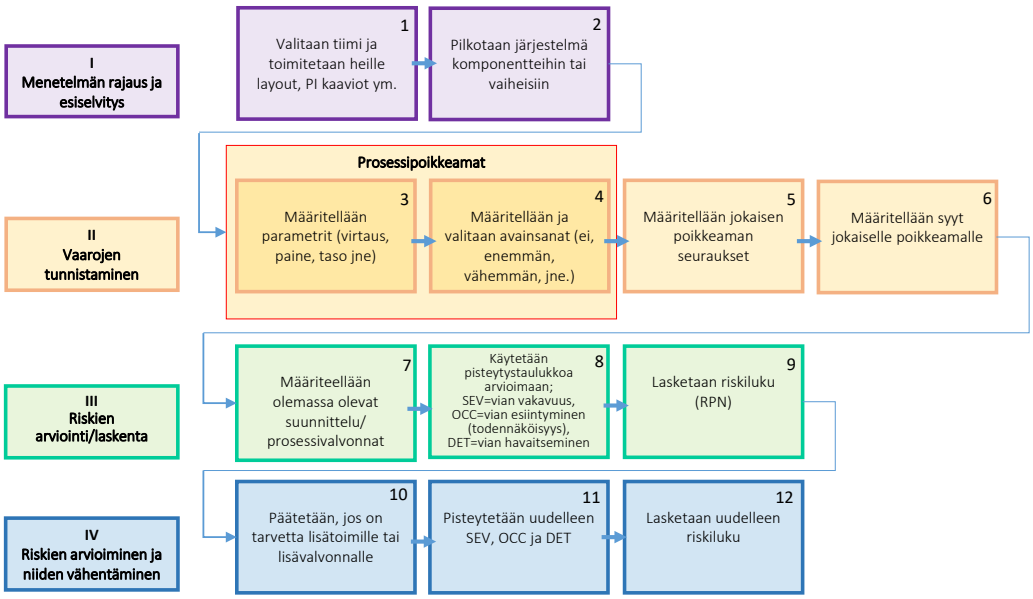
Giardina & Morale (2015) ovat viitanneet Casamirra & kumpp. (2009) julkaisuun jonka mukaan prosessiteollisuuteen on kehitetty monenlaisia vaaran tunnistamisen tekniikoita, mutta ei yksittäistä tekniikkaa, joka voi tunnistaa kaikki turvallisuuden huolenaiheet. Tästä syystä riskinarviointiprosessi voidaan parhaiten saavuttaa järjestelmällisellä lähestymistavalla käyttäen erilaisia tekniikoiden yhdistelmiä. (Giardina & Morale, 2015); (Casamirra;Castaglia;Giardina;& Tomarchio, 2009)

Seuraavissa alakappaleissa käsitellään löytyneitä olemassa olevia menetelmiä ja miten niitä on jo yhdistetty.

5.1.1 Motorolan yhdistetty HAZOP ja FMEA riskienarviointi menetelmä

Motorolassa aikoinaan (2000-luvulla) tietyt ryhmät, kuten ympäristö-, terveys- ja turvallisuus (EHS, Environmental Health and Safety) ja Motorolan tuotantolaitos ovat käyttäneet sekä HAZOP ja FMEA menetelmiä vaihtelevalla menestyksellä. Koska heidän EHS muuttui kohti riskeihin perustuvaa lähestymistapaa päätöksenteossa ja tuotantolaitos kohti luotettavuutta, molemmat organisaatiot etsivät tekniikoita, millä tavoin HAZOP ja FMEA voitaisiin yhdistää. Päätökseen menetelmien yhdistämisestä puolsi myös huomio siitä, että riskianalyysien tekeminen on työlästä ja päällekkäistä työtä tehtiin paljon, koska FMEA ja HAZOP ovat menetelmänä samankaltaisia. Kummankin analyysin tekemiseen kului paljon aikaa ja usein samat henkilöt olivat analyysejä tekemässä, siksipä Motorolalla on kehitetty menetelmää, jolla he saisivat yhdistettyä kummatkin menetelmät yhdeksi kokonaisuudeksi. (Trammell; Lorenzo; & Davis, 2004)

Ensimmäisessä vaiheessa menetelmän eteenpäin viemiseksi tarvitaan ohjaaja, jonka tehtävänä on pitää kasassa tiimi ja ohjata kysymyksillä riskinarviointia oikeaan suuntaan. Itse HAZOP/FMEA tarkasteluprosessi (kuva 16) etenee siten, että valitulle tiimille hankitaan esim. putkitus- ja instrumentointi (PI)- ja sähkösuunnittelukaaviot sekä mahdollinen prosessin ”layout” kuva, joista saadaan kerättyä tarvittavat tiedot. Seuraavaksi prosessi pilkotaan järjestelmä tasolle käsiteltäviin osiin. (Trammell; Lorenzo;& Davis, 2004)



Kuva 16. HAZOP/FMEA prosessin kulku Motorolan tapaan, mukaillen (Trammell;Lorenzo;& Davis, 2004)lähteestä

Toisessa vaiheessa, vaarojen tunnistamisessa, määritellään mitä parametreja (esim. virtaus, paine) ja opassanoja (esim. ei mitään, enemmän, vähemmän) käytetään ja niistä muodostetaan erillinen matriisitaulukko (kuva 17). Edellä mainitut viite- ja opassanat ovat tuttuja HAZOP-analyysimenetelmästä. Motorolan kehittämää matriisitaulukkoa hyödyntäen etsitään/poimitaan prosessipoikkeamat. Kun prosessipoikkeamat on löydetty, jokaiselle poikkeamalle määritellään seuraukset sekä niiden syyt. (Trammell; Lorenzo; & Davis, 2004)

Process Parameter/Guideword Definitions

Process Parameter \ Guideword	None	More	Less	Reverse	Part Of	Other Than	As Well As
Flow	flow stopped	flow greater than specification	flow less than specification	flow opposite specification		flow to wrong location (e.g. spill)	
Level	container empty	container filled above specification (e.g. overflowing)	container filled below specification			loss of containment (e.g. container leaking)	
pH		pH higher than specification	pH lower than specification		pH inconsistent		
Temperature (T)		T higher than specification	T lower than specification				
Pressure (P)	vacuum	P higher than specification	P lower than specification				
State		more phases than specification	fewer phases than specification	change of state		incorrect phases	
Reaction/Addition	no reaction	reaction more rapid than specification	reaction slower than specification	decomposition	reaction stops at intermediate	incorrect reaction product	more reactions than specification
Speed/Frequency	machine action stopped	machine action faster than specification	machine action slower than specification		machine action inconsistent	wrong machine action	
Time (typically for batch process)	process not started	process runs long	process runs short			process starts at wrong time (e.g. out of sequence)	
Composition/Mixing	mixing does not occur	more mixing than specification	less mixing than specification			separation occurs	contamination occurs
Voltage (V)/Current (I)	no electricity flow	V or I higher than specification	V or I lower than specification	current flowing opposite of specification		current to ground	
Information (com)	no com with BPCS (e.g. wires cut)	com faster than BPCS can store	com slower than needed for proper BPCS response		com incomplete	com incorrect	com interference

Kuva 17. Motorolan prosessiparametrien ja opassanojen matriisitaulukko (Trammell;Lorenzo;& Davis, 2004)

Kolmanneksi arvioidaan riskit ja lasketaan ne. Alla olevaan HAZOP/FMEA laskentataulukoon (kuva 18) määritellään olemassa oleville poikkeamille (potentiaalisille vikamuodoille) vian vakavuus ja vaikutus (SEV). Jokaiselle vialle haetaan syyt ja miten ne ovat syntyneet tai mekanismit (OCC) sekä vikamuodon havaitseminen (DET) Motorolan FMEA pisteytystaulukko avulla, joka kuvassa 19.

Motorola's HazOp/FMEA Methodology Worksheet

FMEA WORKSHEET

Issue: 0

PROJECT TITLE _____ Control Number/Issue: _____

FMEA Type: _ Design _ System Company,Group,Site/Business Unit: _____

Prepared By: _____ _____ date _____ (Rev.)

Core Team:

Process Function/ Requirements (Hazop Node / Item)	Potential Failure Mode (Hazop Deviation)	Potential Effect(s) of Failure (Hazop Consequences)	S E V	Potential Cause(s)/ Mechanisms (Hazop Causes)	O C C	Current Design/ Process Controls	D E T	R P N	Recommended Action(s)	S E V	O C C	D E T	R P N

Kuva 18. Motorolan yhdistetty HAZOP/FMEA laskentataulukko. (Trammell;Lorenzo;& Davis, 2004)

Motorola's FMEA Scoring Chart

SCORE	Severity Severity is a rating corresponding to the seriousness of an effect of the potential failure mode. [IN THE ABSENCE OF DETECTION] EHS	Facilities	Occurrence Occurrence is an evaluation of the rate at which a first level cause and the failure mode will occur, with standard preventive maintenance. [1,2,3,4] [IN THE ABSENCE OF DETECTION]	Detection - Process Detection is a rating of the likelihood that the current controls will predict/detect the failure mode and respond to lessen/prevent the consequence. [2,5,6]	Detection - Procedure Detection is a rating of the likelihood that the current controls will predict/detect the failure mode and respond to lessen/prevent the consequence. [7]
1	No effect on people. No regulatory compliance impacts.	No production impact. Process utility in spec. System or equipment or operations failures can be corrected after an extended period.	Failure barely plausible $<1 \times 10^{-6}$ events/hour (1 event in more than 100 years)	Redesign of process eliminating hazard. Rescore RPN for new hazard. *Example: Replacing toxic process chemical with non-toxic chemical.*	Elimination of human based process. *Example: Replace procedure with automated process (which should be separately assessed for risk).*
2	People will probably not notice the failure. Nuisance effects.	No production impact. Process utility in spec. System or equipment or operations failure can be corrected at next scheduled maintenance.	Failure unlikely in similar processes or products. No industry history of failure. $>1x10^{-6}$ events/hour (1 event in 100 years)	Automatic controls highly likely to predict a failure mode and initiate automatic response, preventing the failure mode. *Example: Pressure sensor modifies process conditions to prevent overpressure that would have caused leak.*	Control and release of hazardous energy, with written procedure and independent verification. *Example: Block and bleed of high pressure fluid pipeline, with written procedures and supervisor inspection.*
3	Minor short term irritation effects to people. Moderate, short term non-compliance.	No production impact. Process utility in spec. Equipment or operations failures to be corrected ASAP.	Remote chance of failures. Some industry history. (1 event every couple of decades)	Automatic controls likely to predict a failure mode and initiate manual response, preventing the failure mode. *Example: Pressure sensor activates alarm initiating prepared response plan to prevent overpressure that would have caused leak.*	Control of hazardous energy, with written procedure and independent verification. *Example: Block of high pressure fluid pipeline, with supervisor inspection.*
4	Moderate short term irritation effects to people. Moderate, short term non-compliance.	No production impact. Process utility in spec. Equipment or operations failures to be corrected immediately.	Very few failures likely. $>1x10^{-5}$ events/hour (1 event in 10 years)	Automatic controls likely to detect the failure mode and initiate automatic response, preventing the consequence. *Example: Redundant pH probe in wastewater treatment system, preventing out of control reagent feed.*	Control and release of hazardous energy with written procedures and without independent verification. *Example: Block and bleed of high pressure fluid pipeline, without supervisor verification.*
5	Moderate extended irritation effects to people or environment. Medical intervention needed. Moderate extended non-compliance. Notice of violation (NOV) unlikely.	No production impact. Process utility out of spec. No tool impact. No product scrap.	Few failures likely. Some company history. (1 event every few years)	Manual controls likely to predict the failure mode and initiate manual response, preventing the consequence. *Example: Routine inspection based parametric monitoring program with defined repair program.*	Control of hazardous energy, with written procedure and without independent verification. *Example: Block of high pressure fluid pipeline, without supervisor inspection.*
6	Moderate extended irritation effects to people or environment. Medical intervention needed. Moderate extended non-compliance. NOV likely.	Localized production impact confirmed or likely. Critical process utility out of spec. One or more production tools impacted. Possible product scrap.	Occasional failures. $>1x10^{-4}$ events/hour (1 event per year)	Automatic controls likely to detect the failure mode and initiate automatic response, lessening the consequence. *Example: Ambient air gas sensor activating process shutdown, thereby minimizing leak.*	Cell left blank intentionally to clarify the safety gap between tasks performed with control of hazardous energy and those without control of hazardous energy.
7	Significant but self-recovering effects to people or environment. Moderate extended non-compliance. NOV certain.	Widespread production outage <8 hrs. Critical process utility outage <4hrs or severely out of spec <4 hrs. Product scrap likely.	Moderate number of failures. (1 event every few months)	Automatic controls likely to detect the failure mode and initiate manual response, lessening the consequence. *Example: Exterior leak sensor activates alarm initiating prepared response plan to limit volume of leak.*	No control of hazardous energy, with written procedures and independent oversight. *Example: Electrical hot-work with partner.*
8	Significant but remediable effects to people or environment. Significant long term non-compliance NOV and media attention certain.	Widespread production outage <24 hrs. Critical process utility outage 4-12 hrs or severely out of spec 4-12 hrs. Substantial product scrap likely.	Frequent failures likely. $>1x10^{-3}$ events/hour (1 event every 1.5 months)	Manual controls fairly likely to detect the failure mode and initiate manual response, lessening the consequence. *Example: Routine inspections, with parametric monitoring, with defined measurement thresholds requiring repair.*	No control of hazardous energy, with written procedures and without oversight. *Example: Electrical hot-work without partner.*
9	Probably major injury to people or environment. Regulatory action including fines and process shutdown likely.	Widespread production outage < 48 hrs. Critical process utility outage 12-24 hrs. or moderate contamination of cleanroom or process utility. Substantial product scrap likely.	High number of failures. (1 event every few weeks)	Manual controls might randomly detect failure mode and initiate manual response, lessening the consequence. *Example: Routine walk-by inspections, without parametric monitoring, with defined observed conditions requiring repair.*	Control of hazardous energy, without written procedure.
10	Probably severe injury to people or environment. Regulatory action including fines and process shutdown certain.	Widespread production outage >48 hrs. Critical process utility outage>24 hrs or severe contamination of cleanroom or process utility. Substantial product scrap likely.	Failure certain to occur in near future. $>1x10^{-2}$ events/hour (2 or more events per week)	Controls unlikely to detect the failure mode. *Example: Device fails silent or device not routinely inspected/observed.*	No control of hazardous energy and no written procedures.

1. Failure rates are assumed to apply to continuous processes. Intermittent equipment operational failure rates may be higher due to start up failure, failure to operate at specification, and/or human error.
2. Controls involving design "hardening" (such as stronger materials of construction) are equivalent to QS9000 Type 1 controls and thereby modify Occurrence.
3. If industry average failure rates used and preventive maintenance is less frequent that manufacturer's recommendation, add 1 to Occurrence score.
4. If industry average failure rate used and proven predictive maintenance is utilized, subtract 1 from Occurrence score.
5. Controls that only detect consequence rate a 10 for detection.
6. The reliability of automatic systems and manual procedures is assumed very high. Otherwise, these systems should be assessed separately.
7. The term "hazardous energy" is intended to represent any hazard, including electrical, hydraulic, mechanical (e.g. sharp edge), radiation, chemical, etc.

Cell Color Key:

Inherently safer design/passive controls.
Highest order active controls.
Generally adequate active controls.
Human based active controls.
No controls.

Kuva 19. Motorolassa kehitetty FMEA pisteytystaulukko (Trammell;Lorenzo;& Davis, 2004)

Edellisellä sivulla olevaa FMEA pisteytystaulukkoa on Motorolassa kehitetty usean vuoden ajan. Monet keskeiset käsitteet ovat upotettu taulukkoon, jonka avulla tarkastellaan:

- Vian vakavuutta (SEV). Se on jaettu kahteen osaan; ympäristö- ja henkilöstöturvallisuuden (EHS) ja laitoskokonaisuuden näkökulmasta. EHS käsittää esim. henkilön loukkaantumiset, ympäristötuhot, negatiivisen julkisuuden ja sanktiot. Laitoskokonaisuus sisältää tuotevauriot, prosessikatkot, laitosvauriot ja toiminnalliset katkokset.
- Esiintyminen (OCC) on arvio siitä, millä tiheydellä/tahdilla syy-seuraus ja vikamuoto esiintyvät (vikamuodon ja poikkeaman esiintymistiheys).
- Havaitseminen (DET) on laskennallinen todennäköisyys, jolla havaitaan ja hallitaan tai estetään vikamuoto, joko estämällä vikamuodon syy tai minimoimalla vian seuraukset, ennen kuin se vaikuttaa henkilöön, prosessiin tai laitokseen. DET arvio on myös hyödyllinen silloin, kun arvioidaan henkilöjärjestelmien toimivuutta työturvallisuuskartoituksissa tai onnettomuustutkinnoissa.

(Trammell;Lorenzo;& Davis, 2004) ovat sitä mieltä, että heidän kehittämällään tehokkaalla yhtenäisellä riskinarvioinnin lähestymistavalla varmistetaan, että riittävä valvonta toteutetaan johdonmukaisesti sekä hallitaan koko laitoksen riskejä siedettävällä tasolla.

5.1.2 Yhdistetty FMECA ja HAZOP eli FHIA

Giardina & Morale (2015) ovat yhdistäneet FMECA ja HAZOP menetelmät työkaluksi, jota kutsutaan FHIA:ksi (FMECA and HAZOP Integrated Analysis).

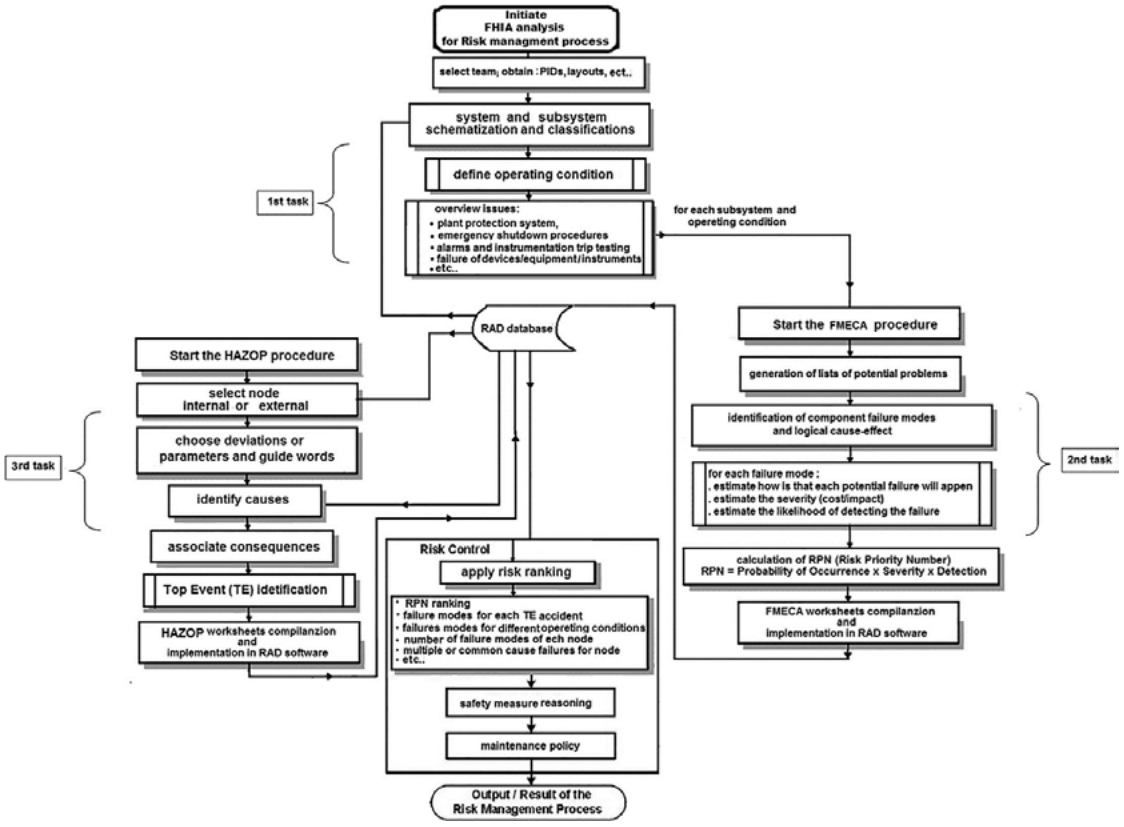
FHIA on suunniteltu työkaluiksi, jonka avulla voidaan kerätä sekä järjestää prosessista saatuja luotettavuus- ja riskitietoja enemmän kuin mitä yhden riskianalyysimenetelmän avulla saataisiin. Työkalu kehitettiin, kun turvallisuusanalyysi tehtiin mahdollisten satunnaisten tapahtumien määrittämiseksi nestemäisen maakaasun varastoinnille. FHIA menetelmää on sovellettu Italiassa vuonna 2014 rakenteilla olevan Porto Empedoclen nestemäisen maakaasun LNG-varastointijärjestelmän riskianalyysiin. Analyysia tuettiin käyttäen uutta riskianalyysitietokantaohjelmaa RAD (Risk Analysis Database), joka on kehitetty Energia-, Informaatiotekniikan ja Matemaattisten mallien (Department of Energy, Information Engineering and Mathematical Models (DEIM), laitoksella, Palermon yliopistossa Italiassa. Heidän tavoitteena on FHIA:n soveltamisen standardointi. (Giardina & Morale, 2015)

Tutkijoiden mukaan yksityiskohtaiset kuvaukset mahdollisista onnettomuustilanteista ja komponenttihäiriöistä sekä onnettumomuusjaksoista, ja riippuvuudet laitteiden ja ihmisten toiminnnan välillä, voidaan saavuttaa soveltamalla FHIA menetelmää. (Giardina & Morale, 2015)

Eri käyttöolosuhteissa ja tarkastellun prosessin eri vaiheissa tehtävä tarkastelu antaa loogisemmat syyt laitevikoihin ja epätoivottaviin seurauksiin eli huipputapahtu-

miin (TE, Top Events). Edellä mainittu on erittäin vaikea tehtävä erityisesti niissä teknologioissa, joille on ominaista suuri määrä prosesseja samalle alijärjestelmälle. Toisekseen FHIA tarjoaa kattavan luettelon tapahtumista tai tapahtumien yhdistelmistä, jotka vaikuttavat samoihin tai erilaisiin TE: iin. Tämän ansiosta voidaan keskittyä vaaran kriittisiin pisteisiin ennen kvantitatiivista arviointia esiintymistodennäköisyydestä. Koska inhimilliset virheet ovat onnettomuuksien yleisimmin tunnistetut syyt, RPN (Risk priority number) -indeksin avulla voidaan luokitella sekä komponenttihäiriöt että ihmisen virheet. Tulosten avulla voidaan LNG-varastointimenetelmistä kerätä huomattava määrä tietoa, mikä voi olla hyödyllistä suunniltaessa huoltotoimenpiteitä tai asianmukaista turvallisuusvalvontaa. (Giardina & Morale, 2015, s. 36)

Menetelmä on jaettu kolmeen päävaiheeseen, kuten kuvassa 20 on esitetty.



Kuva 20. FHIA analyysin kulku (Giardina & Morale, 2015, s. 38)

Ensimmäisessä vaiheessa turvallisuusanalyytikoilla ja suunnittelun asiantuntijoilla on oltava tarkka kuvaus laitoksesta ja prosessista (prosessin virtakaaviot, putkisto- ja instrumentointikaaviot (PI); komponenttien luotettavuustiedot, tiedot turvalaitteista sekä prosessin turvallisesta alasajosta, käyttö ohjeet, prosessin raja-arvot). Myös operatiiviset tehtävät, kuten käyttö- ja kunnossapitomenetelmät, tarkastukset jne. käy-

dään tarkastelussa läpi. Prosessi pilkotaan siten useaan osajärjestelmään ja jokaisesta osajärjestelmästä kuvataan sen toiminta. (Giardina & Morale, 2015)

Toisessa vaiheessa ryhmä listaa FMECA-laskentataulukoon (toteutetaan RAD –ohjelmistossa) jokaisen osajärjestelmän laitteet tai komponenetit ja luetteloi niiden mahdolliset ongelmat. Seuraavaksi tunnistetaan komponenttien vikatilanteet ja niiden syy-seuraus suhde. Kullekkin vikatoiminnalle arvioidaan; miten jokainen potentiaalinen vika esiintyy (O), vian vakavuus (S) kustannus/vaikutus huomioon ottaen sekä vian todennäköisyys (D). Edellämainituille kolmelle kohdalle lasketaan riskiprioriteetti numero RPN, kaavalla O*S*D.

RPN-luokitteluasteikko on välillä 1 ja 1000 ja prioriteetit toimenpiteille ovat seuraavasti:

- Erittäin alhainen, jos RPN <5 (lähes tarpeetonta ryhtyä jatkotoimiin),
- Alhainen, jos 5 <RPN <20 (vähäinen prioriteetti ryhtyä jatkotoimiin),
- Keskitaso, jos 20 <RPN <200 (kohtalaisen tärkeä ryhtyä jatkotoimiin),
- Korkea jos 200 <RPN <500 (ensisijaisen ryhtyä jatkotoimiin),
- Erittäin korkea, jos RPN> 500 (ehdottoman välttämätöntä ryhtyä jatkotoimiin). (Giardina & Morale, 2015)

Koska perinteisissä FMECA-sovelluksissa ei pystytä käsittelemään inhimillisiä virheitä; siksi tässä menetelmässä ehdotettiin ihmisvirheen sisällyttämistä esiintymisparametriin O (Occurrence). Alla olevassa taulukossa 15 esitetyt arvot ovat esiintyvyysjärjestys komponenttihäiriöille ja inhimillisten virheiden todennäköisyydelle. (Giardina & Morale, 2015)

Taulukko 15. Asteikko komponenttihäiriöiden ja inhimillisten virheiden todennäköisyydelle. (Giardina & Morale, 2015)

Component failure occurrence probability (operating day)		Human error occurrence probability	Rank
Unlikely, unreasonable to expect failure to occur,	<1:20,000	Less than every 5 years	1
Low failure rate,	1:20,000	In 3–5 years,	2
	1:10,000	In 1–3 years	3
Occasional failures,	1:2000	Per year	4
	1:1000	In 6 months	5
	1:200	In 3 months	6
Repeated failures,	1:100	Per month	7
	1:20	Per week	8
Inevitable failure, almost certain to cause problems	1:10	Every few days	9
	1:2	Per day	10

Taulukossa 16 on esitetty vakavuusluokitus vian tai virheen vaikutukselle sekä taulukossa 17 todennäköisyysluokitus vian tai virheen havaitsemiselle.

Taulukko 16. Vian tai virheen vaikutuksen vakavuusluokitus (Giardina & Morale, 2015)

Severity of each effect of failure or error	Effect	Rank
No reason to expect failure to have any effect on safety, health, environment or mission	None	1
Very minor effect on product or system performance to have any effect on safety or health. The system does not require repair.	Very Minor	2
Minor effect on product or system performance to have any effect on safety or health. The system can require repair.	Minor	3
Very low effect on system performance. A failure is not serious enough to cause injury, property damage, or system damage, but can result in unscheduled maintenance or repair.	Low	4
Moderate effect on system performance. The system requires repair. A failure which may cause moderate injury, moderate property damage, or moderate system damage which will result in delay or loss of system availability or mission degradation. 100% of mission may need to be reworked or process delayed.	Moderate	5
System performance is degraded. Some safety functions may not operate. A failure causes injury, property damage, or system damage. Some portion of mission is lost. High delay in restoring function.	Significant	6
System performance is severely affected but functions (reduced level of safety performance). The system may not operate. Failure does not involve noncompliance with government regulations or standards.	Major	7
System is inoperable with loss of primary function. Failure can involve hazardous outcomes and/or noncompliance with government regulations or standards.	Extreme	8
Failure involves hazardous outcomes and/or noncompliance with government regulations or standards. Potential safety, health or environmental issue. Failure will occur with warning.	Very extreme	9
Failure is hazardous and occurs without warning. It affects safe operation. A failure is serious enough to cause injury, property damage, or system damage. Failure will occur without warning.	Serious	10

Taulukko 17. Todennäköisyys vian tai virheen havaitseminen (Giardina & Morale, 2015)

Likelihood of detection of failure or error	Degree of importance	Probability of failure detection %	Rank
Current control(s) almost certainly will detect a potential failure mode/task error. Reliable controls are known with similar process.	Almost certain	0–5	1
Very likelihood current control(s) will detect failure modes/task error. Controls are able to detect within the same machine/module (almost always preceded by a warning).	Very high	5–15	2
High chance the design control(s) will almost certainly detect a potential failure mode/task error. Controls are able to detect within the same function area.	High	15–25	3
Moderately high likelihood current control(s) will detect failure modes/task error.	Moderately high	25–35	4
Moderate chance that the design control will detect a potential failure mode/task error, or the defect will remain undetected until the system performance is affected.	Moderately	35–45	5
Low likelihood current control(s) will detect failure modes/task error (program or operator is not likely to detect a potential design weakness).	Low	45–55	6
Very low likelihood current control(s) will detect failure modes/task error (program or operator will not to detect a potential design weakness).	Very low	55–65	7
Remote chance that the design control will detect a potential failure mode/task error, or the defect will remain undetected until an inspection or test is carried out.	Remote	75–85	8
Defect most likely remains undetected (very remote chance that the design control will detect a potential cause/mechanism and subsequent failure modes) or the task will be performed in the presence of the defect.	Very remote	85–95	9
System failures are not detect (design control will not and/or cannot detect a potential cause/mechanism and subsequent failure modes) or there is no design verification or the task will certainly be performed in the presence of the defect.	Almost impossible	90–100	10

Kolmas vaihe on HAZOP tarkastelu ja tiimi keskittyy kunkin osajärjestelmän tiettyihin pisteisiin, joita kutsutaan sisäisiksi ja ulkoisiksi solmuiksi. Kussakin näistä solmuista prosessiparametrien poikkeamat tutkitaan käyttämällä HAZOP menetelmästä tuttuja ohjaussanoja. Tehtävän suorittamiseksi laitevioille tai inhimillisille virheille tunnistetaan syyt ja niiden seuraukset ja lisätään HAZOP-laskentaan. Jokaiselle huipputapahtumalle (jotka on tunnistettu HAZOP-menettelyn kautta) kriittiset syyt luokitellaan saaden niille RPN arvo. (Giardina & Morale, 2015)

FMECAn ja HAZOPin yhdistetyn analyysin (FHIA) edut:

- Lähestymistapa voi vähentää merkittävästi subjektiivisia tekijöitä, jotka johtuvat tiedon puutteesta ja joka tekee analyytikoille mahdollisuuden tehdä monia yksinkertaistuksia.
- Laskee; kuinka monta kertaa vikamuodot (poikkeaman syyt) esiintyvät (FMECA analyysin avulla) sekä HAZOP analyysin avulla tunnistettuja vahinkotapahtumia (seurauksia). Tämä voidaan suorittaa jokaiselle toimintaolosuhteelle
- tunnistaa useita virheitä, jotka vaikuttavat jokaiseen järjestelmään tai naapurijärjestelmiin
- listaa kriittiset vikatyypit jokaisesta huipputapahtumasta
- ryhmitelee laskentataulukot jokaiselle solmulle, esimerkiksi
    - fyysinen parametri (virtaus, paine, lämpötila, taso, jne.),
    - poikkeaman tyyppi (enemmän kuin, vähemmän kuin jne.),
    - poikkeaman syy (vikamuodot tai inhimilliset virheet) ja
    - huipputapahtumat (TE = Top Events)
- tukee analyytikoita turvallisuusanalyysin versioinnissa ja pitämään sen ajan tasalla, koska menetelmä esimerkiksi:
    - tutkii eri solmupisteitä eri alijärjestelmien samankaltaisissa prosesseissa
    - lataa turvallisuustietoja (käyttöturvallisuustitiedot) samoista komponentista, joita käytetään eri kokoonpanoissa
    - menetelmän avulla voidaan suorittaa muutoksenhallinta eli Management of Change (MOC) -menettely, ja
    - auttaa päätöksentekijöitä valitsemaan asianmukaiset turvatarkastukset ja suunnittelemaan kunnossapidon menettelyt
- kerää huomattavan määrän tietoja koskien tarkasteltavan laitoksen prosesseja ja turvallisuutta. (Giardina & Morale, 2015, ss. 37 - 38)

Tulokset osoittivat, että FHIA on hyödyllinen tekniikka, jolla tunnistetaan paremmin ja johdonmukaisemmin ihmisen virheiden mahdolliset lähteet, virheiden syy-tekijät, moninkertaiset tai yleiset syyongelmat ja vaaratekijöiden syy-seuraus korrelaatio prosessin eri vaiheista. (Giardina & Morale, 2015, s. 44)

5.1.3 Yhdistelmä HAZOP- ja RCM II- menetelmistä

HAZOPin ja RCM:n vaiheittain etenevät analysointimenetelmät hukkaavat organisaatiossa arvokasta aikaa ilman hyötyjä. (Clarke & Young, 2011) kyseenalaistavat artikkelissaan luotettavuuskeskeinen kunnossapito (RCM) ja HAZOP - onko tarvetta molemmille menetelmille, koska niiden välillä on hyvin paljon yhtäläisyyksiä. Yhtäläisyyden on lueteltu taulukossa 18. Kunkin prosessin tuotosten tarkastelu osoittaa, että HAZOP-tutkimuksen loppuun saattaminen ei tarjoa RCM-analyysille hyötyjä. Toisaalta RCM II -analyysin loppuun saattaminen tuottaa olennaisesti HAZOP-tutkimukseen tuloksia. (Clarke & Young, 2011)

Taulukko 18. HAZOP- ja RCM menetelmien samankaltaisuudet (Clarke & Young, 2011)

Activity or Outcome	HAZOP	RCM	Comment
Project definition and planning	Yes	Yes	The objectives and scope of the study are defined, and potential team members identified
Detailed preparation and planning	Yes	Yes	All design and other documentation relating the analysis are gathered, including PIDs, drawings, operating and maintenance manuals, etc. Functional breakdown and defining of system boundaries for analysis, estimation of duration, and development of analysis schedule are also performed
Training for team members	Yes	Yes	The Aladon RCM II training course has been delivered and developed over the last 20 years in more than forty countries and is widely regarded as setting the benchmark in SAE JA-1011 compliant RCM training
Team comprises operations and maintenance people working together	Yes	Yes	Both processes use people who know the process best including operations and maintenance people and technical specialists as required
Analysis managed by highly trained Facilitator	Yes	Yes	The facilitator in both cases needs to have a comprehensive understanding of their methodology and be able to facilitate the analysis group.
Documentation of the plant process	Yes	Yes	*The Failure Modes and Effects Analysis (FMEA) of the RCM II analysis is functionally based and therefore documents how the users intend the plant to operate. The process documents the failed states and captures all likely failure modes, including those which may be operator induced, those which result from the failure or degradation of plant components and failures which are the result of the plant's inability to perform as required, i.e. design errors.* *Note: IEC 61882 standard suggests in paragraph 5.2 that FMEA is a component based analysis (as described in IEC 60812) and hence can not be used for process analysis. However, FMEA (and FMECA) can be functionally based, as described in other widely used standards such as MIL-STD-1629(A) and therefore can also be process based. The FMEA used in an RCM II analysis is functionally based, not component based*
Documentation of the ways in which the plant can fail	Yes	Yes	The RCM process does not formally use the HAZOP style guide words for defining Functional Failures. However, Functional Failures describe the failed states of the system in the same manner, and guide words can be used
Documentation of the possible failure modes	Yes	Yes	HAZOP lists failure modes to cover human error and process error and groups failure modes which result in a common effect together, e.g., pump impeller worn, pipe work partially blocked, leakage etc RCM lists all likely failure modes including human error and keeps failure modes with common effects separated to allow failure management policies to be developed
Documentation of failure consequences	Yes	Yes	In RCM terms, HAZOP uses free text and the Facilitator to define the Failure Effects. The RCM FMEA uses free text to describe the failure symptoms and the effort needed to correct the failure and secondary damage. (Called Failure Effects). Failure consequences are later defined by the RCM decision logic as Hidden, Safety/Environmental, Operational, Non Operational. Failure management strategies are developed according to the failure consequences
Identification Safeguards	Yes	Yes	HAZOP utilizes a column on the worksheet to document any safeguards for a particular hazard. In FMEA/RCM, safeguards are documented in the Failure Effects column to ensure the analysis team is aware of the safeguards during the development of risk management strategies. RCM includes safeguards as a function eg, "To provide an alarm in the event the pressure exceeds 250kPa"
Development of design change recommendations to address process shortfalls	Yes	Yes	
Development of risk management (maintenance) strategies	No	Yes	RCM takes to conclusion the development of strategies to manage the identified risk. Strategies include the proactive maintenance tasks of On Condition Maintenance, Scheduled Restoration and Scheduled Discard. In the event the failure can not be prevented, management strategies work to minimize the failure consequences including Failure Finding and Redesign. No Scheduled Maintenance is an option for failures where the failure of the component or asset is tolerable
Development of maintenance task intervals based on risk and consequence	No	Yes	RCM utilizes a robust process to define the most appropriate management strategy based upon the failure characteristics. In the event a failure can not be prevented by a proactive task and the failure has hidden consequences, the interval for the functional check of the device is determined based upon a mathematical equation linking risk and consequence. Risk is determined by the demand rate for the device and the probability the item will be in failed state when required

Document actions required	Yes	Yes	HAZOP defines the task required to correct the failed state from an operational perspective. RCM defines the task and frequency of the task to ensure the function of the asset is maintained, be it operational, maintenance, engineering redesign, operational procedures, training, etc
Task allocation	Yes	Yes	
Development of asset maintenance strategies	No	Yes	
Development of Fault Finding Guide	No	Yes	RCM utilizes the Failure Effects information to populate a key word symptom driven fault finding guide

HAZOPin ja RCMn välillä on eroja toteutettavissa toimenpiteissä. Esimerkkinä HAZOPista puuttuvat toiminnat:

- Kunnossapidon riskinhallinnan strategioiden kehittäminen
    - Tunnistetun riskin hallitsemiseksi RCM avulla voidaan kehittää strategioita. Strategiat sisältävät kunnonvalvonnan ennakoivan kunnossapidon tehtävissä, ennakoivien huoltotehtävien visuaalisen/automaattisen tarkastuksen ja kohteen poistamisen käytöstä määrätyn aikarajan jälkeen. Jos vikaantumista ei voida estää, kunnossapitostrategialla pyritään minimoimaan vikaantumisen seuraukset sekä myös vianetsintä ja uudelleensuunnittelu. Aikatauluttamaton kunnossapito on mahdollinen vikoihin, joissa osan tai laitteen vikaantuminen on sallittua. (Clarke & Young, 2011)
- Kunnossapidon tehtävien jaksotus perustuen riskeihin ja seurauksiin
    - RCM hyödyntää prosessia määrittelemään kunnossapitostrategiaa, joka perustuu vikojen erityispiirteisiin. Mikäli vikaa ei voi estää ennakoivalla toiminnalla ja vialla on piilossa olevia seurauksia, aikaväli laitteen toiminnalliselle tarkastukselle on määritelty perustumaan matemaattisiin yhtälöihin yhdistäen samalla riskin ja seurauksen. Riski on määritelty laitteen vaatimustason mukaan ja todennäköisyys, että laite on vikatilassa. (Clarke & Young, 2011)
- Laitteiden kunnossapitostrategioiden kehittäminen
- Vikahakuohjeen kehittäminen
- RCM hyödyntää vian vaikutuksien tietoa täydentäen siten avainsanoja vianhakuohjeeseen. (Clarke & Young, 2011)

HAZOP-analyysissä käytetään sovittuja ”opassanoja” mahdollisten poikkeamien tunnistamiseksi. Opassanat ovat mm: ei tai ei mitään, enemmän, vähemmän, lisäksi, osittain, päinvastoin, muu kuin, aiemmin, myöhemmin, ennen ja jälkeen. Esimerkiksi opassana ”vähemmän” tapauksessa pohditaan, mitä jokin määrällinen lasku voi aiheuttaa järjestelmässä oikeaa arvoa alemman virtauksen tai paineen. Tyypillinen HAZOP-dokumentti esitettynä kuvassa 19. (Clarke & Young, 2011)

Taulukko 19. IEC 61882 standardissa kuvattu tyypillinen HAZOP-dokumentti (Clarke & Young, 2011)

STUDY TITLE: PROCESS EXAMPLE							SHEET: 2 of 4		
Drawing No.:		REV. No.:					DATE: December 17, 1998		
TEAM COMPOSITION:		LB, DH, EK, NE, MG, JK					MEETING DATE: December 15, 1998		
PART CONSIDERED:		Transfer line from supply tank A to reactor							
DESIGN INTENT:		Material: A Source: Tank for A		Activity: Destination:		Transfer continuously at a rate greater than B Reactor			
No	**Guide word**	**Element**	**Deviation**	**Possible causes**	**Consequences**	**Safeguards**	**Comments**	**Actions required**	**Action allocated to**
4	MORE	Transfer A	More transfer Increased flow rate of A	Wrong size impeller Wrong pump fitted	Possible reduction yield Product will contain large excess A	None		Check pump flows and characteristics during commissioning Revise the commissioning procedure	JK
5	LESS	Material A	Less A	Low level in tank	Inadequate net positive suction head Possible vortexing and leading to an explosion Inadequate flow	None	Unacceptable Same as 1	Low-level alarm in tank Same as 1	MG
6	LESS	Transfer A. (at rate >B)	Reduced flow rate of A	Line partially blocked, leakage, pump under-performing, etc.	Explosion	None shown	Not acceptable	Same as 2	JK

Järjestelmän toiminnot; vikaantuminen, vikamuoto (syy) ja vikaantumisen vaikutukset määritellään vika-, vaikutusanalyysissä (FMEA), johon RCM-päätöslogiikkaa on sovellettu. John Moubrayn kehittämässä RCM II:ssa, tiedonkeruumenetelmänä käytetään FMEA-analyysiä, josta esimerkki taulukossa 20. RCM II tunnistaa prosessitoiminnot ja virheet, jotka voivat vaikuttaa prosessin suorituskykyyn. Tunnistetut vikaantumiset voivat johtua laitteen toimintahäiriöstä, laitteiden huonontumisesta, inhimillisistä virheistä sekä sopimattomasti tai virheellisesti suunnitellusta tai asennetusta laitoksesta. RCM II -prosessin tavoitteena on löytää sopivin tapa hallita jokainen näistä riskeistä. (Clarke & Young, 2011)

Taulukko 20. RCM II tiedonkeruumenetelmänä oleva FMEA taulukko (Clarke & Young, 2011)

RCM II INFORMATION WORKSHEET © 1994 Aladon Ltd	SYSTEM	*Southwest water reticulation system*	No. 0	Compiled by TAP	Date 04-Jul-05	Sheet *1*
	Sub-SYSTEM	*North East Pipeline*	Ref. AC *Pipeline*	Reviewed by MCW	Date	of 3

FUNCTION		FUNCTIONAL FAILURE		FAILURE MODE (Cause of failure)		FAILURE EFFECT (What happens when it fails)
1	To supply a 'Normal' service connection with potable water (to ADWG std) at a flow rate of not less than 0.06 litres per second at a pressure not less than 120 kpa through AC pipe to a section that can be isolated to less than 20 services	A	Unable to supply at all	1	Material failure due to manufacturing fault	Failure occurs under normal operation of the pipeline and would reduce the useful life of the asset. May be indicated by a small leak. Failure results in loss of supply to up to 20 normal services. Downtime to repair 8 hours at a cost of $8000
1		A		2	Pipeline corrodes to the point of failure	Failure occurs under normal operation of the pipeline and would reduce the useful life of the asset. Failure results in loss of supply to up to 20 normal services. Downtime to repair 8 hours at a cost of $8000
1		A		3	Pipe line crushed when external load exceeds design	Failure occurs under normal operation of the pipeline and would reduce the useful life of the asset. Failure results in loss of supply to up to 20 normal services. Downtime to repair 8 hours at a cost of $1,000
1		A		4	Pipeline fails from fatigue during normal operation	Failure occurs under normal operation of the pipeline and would reduce the useful life of the asset. Usually ruptures without warning but usually in response to a change in system pressure or cyclic external forces. May be indicated by a small leak. Failure results in loss of supply to up to 20 normal services. Downtime to repair 8 hours at a cost of $8,000

Artikkelissa kerrotaan, kuinka joitain HAZOP-menetelmän osia sisällytetään FMEA / RCM-analyysiin - molempien analyysimenetelmien tavoitteet voidaan olennaisilta osiltaan täyttää mahdollisimman pienillä muutoksilla ja panoksilla.

Lisäämällä ja käyttämällä RCM II -menetelmässä tunnettuja HAZOP-opas-sanoja, itse HAZOP menetelmästä tulee vielä selvempi ja RCM II:kään ei vaarannu. HAZOP:ssa generoituneet mahdolliset syyt (taulukon kohta ”possible causes”) luetellaan RCM II -analyysissä kohdassa vikamuoto (failure mode). Lopputulemana HAZOP opas-sanoista ja RCM II toiminnallisista vikaantumisista koostettu taulukko 21, joka on esitettynä alla. (Clarke & Young, 2011)

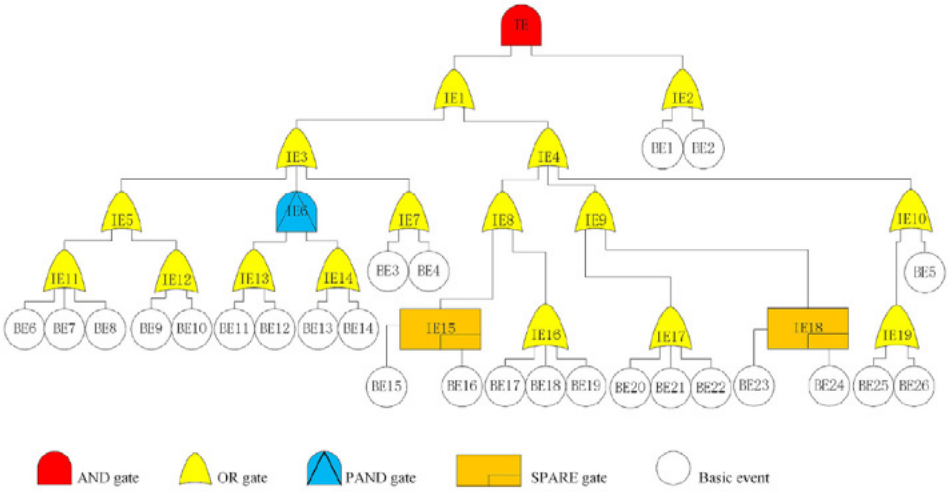
Taulukko 21. HAZOP opassanat ja RCM II toiminnaliset vikaantumiset (Clarke & Young, 2011)

Derivation	Guide Word	Example interpretation from process industry	Example interpretation for a Programmable Electronic System PES	RCM II Typical Functional Failure Wording (in response to appropriate Function definition)
Negative	No	No part of the intention is achieved e.g. no flow	No data or control signal	Unable to provide flow at all
Quantitative modification	More	A quantitative increase e.g. higher temperature	Data is passed is passed at a higher rate than intended	Temperature greater than "x" deg C
	Less	A quantitative decrease e.g. lower temperature	Data is passed at a slower rate than intended	Temperature less than "y" deg C
Qualitative modification	As well as	Impurities present Simultaneous execution of another operation/step	Some additional or spurious signal is present	Allows product contamination Enables simultaneous operation of plant process
	Part of	Only some of the intention is achieved, i.e. only part of an intended fluid transfer takes place	The data or control signals are incomplete	Unable to complete fluid transfer within "x" minutes
Substitution	Reverse	Covers reverse flow in pipes and reverse chemical reactions	Normally not relevant	Allows reverse flow in pipework
	Other than	A result other than the original intention is achieved, i.e. transfer of wrong material	The data in control signals are incorrect	Allows wrong material to be transferred
Time	Early	Something happens early relative to clock time, e.g. cooling or filtration	The signals arrive too early with reference to clock time	Initiates cooling too early
	Late	Something happens late relative to clock time, e.g. cooling or filtration	The signals arrive too late with reference to clock time	Initiates cooling too late
Order or sequence	Before	Something happens too early in a sequence, e.g. mixing or heating	The signals arrive earlier than intended within a sequence	Initiates mixing too early
	After	Something happens too late in a sequence, e.g. mixing or heating	The signals arrive later than intended within a sequence	Initiates mixing too late

5.1.4 Laajennettu HAZOP tarkastelu dynaamisella vikapuu analyysillä eli DFT:llä

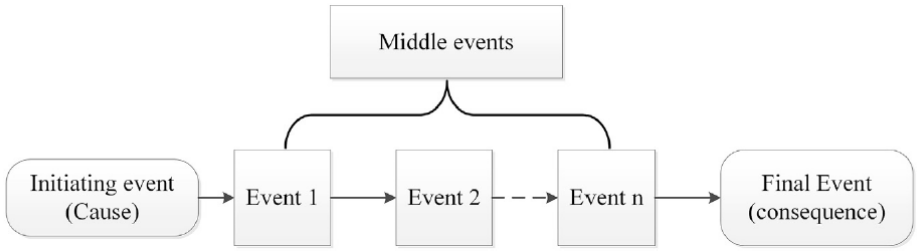
Julkaisun (Guo & Kang, 2015) tulokset osoittavat, että verrattaessa tavanomaista HAZOP lähestymistapaa heidän ehdottamaansa laajennettuun HAZOPiin, jossa mukana dynaaminen vikapuu analyysi (dynamic fault tree, DFT), se tunnistaa tehokkaasti vian juurisyyt, määrittelee määrällisesti huipputapahtuman todennäköisyyden ja todennäköisimmät vian aiheuttajat. Laajennettu HAZOP lähestymistapa tuottaa luotettavan pohjan kemikaalitehtaan prosessiturvallisuuden parantamiseen.

Koska perinteinen vikapuu-menetelmä ei arvioi aikaansidottujen monimutkaisten järjestelmien vikakäyttäytymistä, menetelmää kehitettiin lisäämällä uudet dynaamiset logiikkaportit. DFT sisältää vikapuun, joka sisältää ainakin yhden erityisen dynaamisen logiikkaportin, kuten (Priority And, PAND) portin, sekvenssiä vahvistavan portin (sequence enforcing gate, SEQ), SPARE-portin ja toiminnallisen riippuvuuden (functional dependency, FDEP) portin (kuva 21). Tällätavoin pystytään kuvaamaan graafisesti ja hierarkkisesti kaikkia virheellisten laitteiden syy-seuraussuhteita. (Guo & Kang, 2015)



Kuva 21. Esimerkki dynaamisesta vikapuusta (Guo & Kang, 2015)

Laajennettu HAZOP menetelmä (kuva 22) etenee seuraavanlaisesti:
Ensimmäiseksi suoritetaan tavanomainen HAZOP menetelmä. Kun tiedot mm. PI kaavioista, prosessin vuokaavioista, käyttötavoista ja mahdollisisita aiemmista prosessiturvallisuustarkastuksista on kerätty, analysoitu laitos jaetaan osiin, joita kutsutaan solmuiksi. Tietyille solmuille määritellään poikkeamat, jotka koostuvat prosessiparametreistä kuten lämpötila, paine ja virtaus sekä opassanat esim. ei tai ei mitään, enemmän, vähemmän jne. Tämän jälkeen poikkeamille tunnistetaan mahdolliset vian syyt ja niistä aiheutuvat seuraukset. (Guo & Kang, 2015)

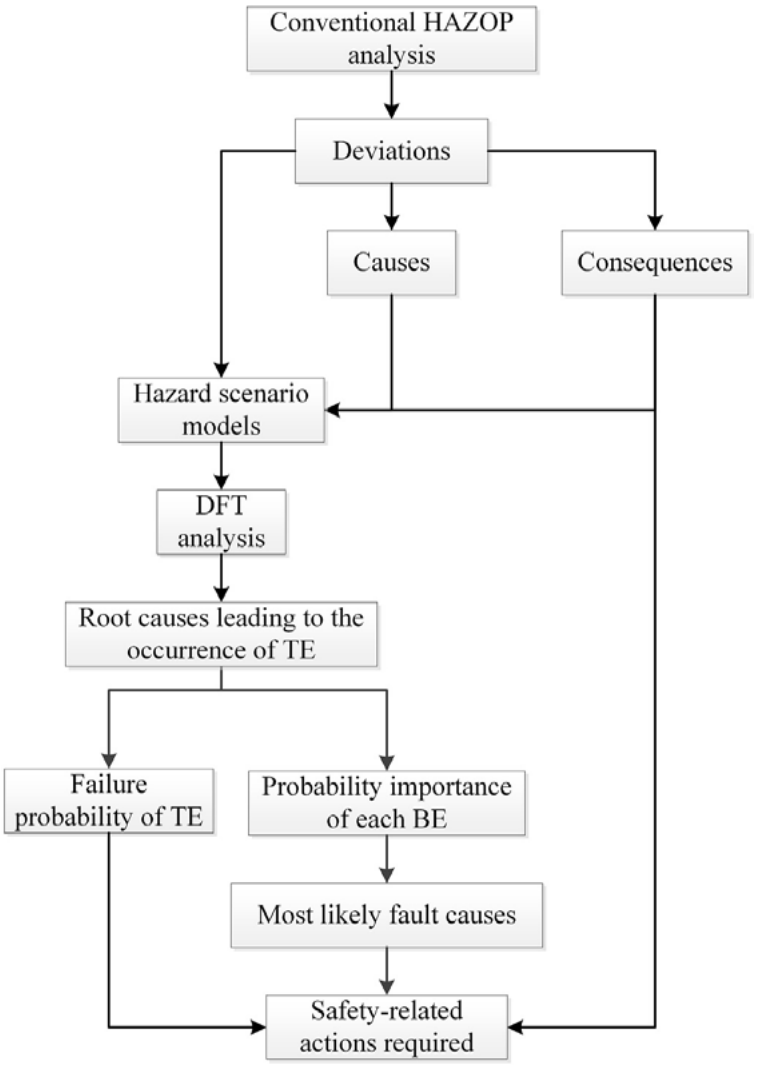


Kuva 22. Riskiskenaariomalli (Guo & Kang, 2015)

Koska poikkeamilla voi olla useita vikaantumisia ja erilaisia seurauksia, HAZOP-analyysituloksen muuntaminen suoraan DFT-malliksi on monimutkaista ja vaikeaa. Tästä syystä on välttämätöntä rakentaa riskiskenaariomalli (kuva 23). Se on vian etenemisprosessi, vikaketju, jossa vian alkuperästä syystä päästään vian seuraukseen. Riskiskenaariomalleihin perustuen suoritetaan myöhemmin dynaaminen vikapuuanalyysi, jossa huipputapahtumana on riskiskenaariosta saatu lopputapahtuma. Osi-

en tai laitteiden kompponentti tasolla tunnistetaan viat, jotta niillevoidaan määrittää juurisyyt. (Guo & Kang, 2015)

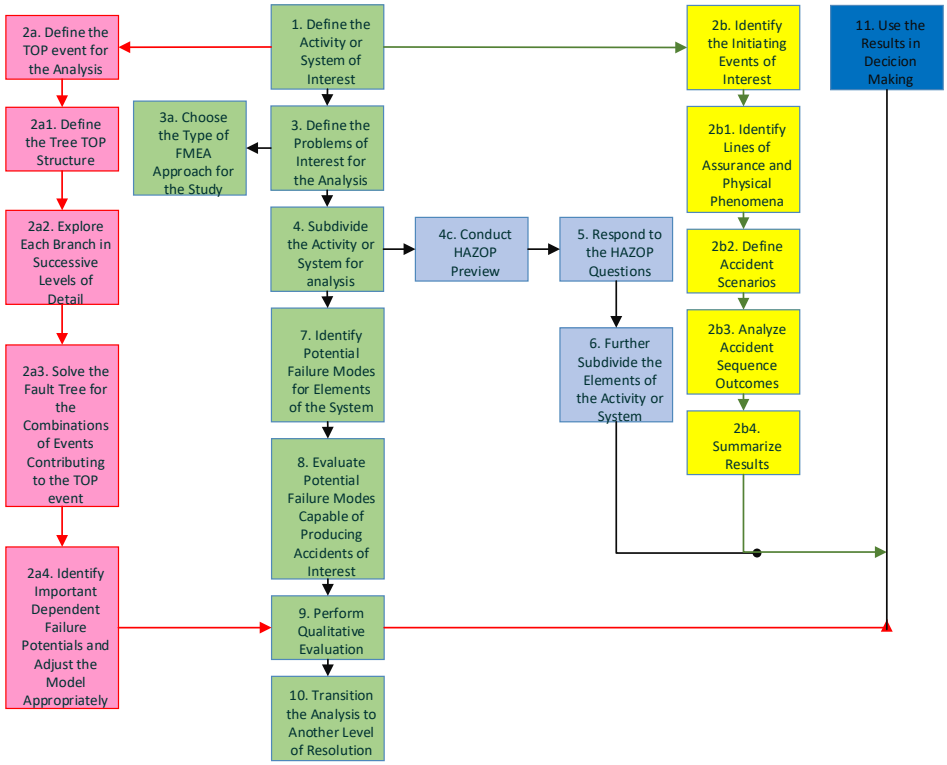
Dynaamisen vikapuumallin avulla määritetään määrällinen analyysi, jossa lasketaan huipputapahtuman (top event, TE) vikaantumisen todennäköisyys ja kunkin perustapahtuman (basic event, BE) todennäköisyysarvot. Siten saadaan riskijärjestys, jolla voidaan turvallisuuteen liittyvä heikoin kohta tunnistaa. Lopuksi voidaan ehdottaa sopivia turvallisuuteen liittyviä toimenpiteitä prosessin turvallisuuden varmistamiseksi tai parantamiseksi laitoksen elinkaaren aikana. (Guo & Kang, 2015)



Kuva 23. Laajennetun HAZOP analyysimenetelmän kulku (Guo & Kang, 2015)

5.1.5 Yhdistetty HAZOP, FMEA, FTA ja ETA

Silvianita et al. (2011) mukaan jokaisella riskianalyysitekniikalla on omat rajoituksensa, siksi monet tutkijat ovat yhdistäneet eri menetelmiä. Tutkijat ovat yhdistäneet neljä eri riskienhallintamenetelmää, joita ovat HAZOP, FMEA, vikapuuanalyysi (Fault Tree Analysis, FTA) ja tapahtumapuuanalyysi (Event Tree Analysis, ETA). Havaittiin, että em. riskienarviointimenetelmät voidaan integroida uutena lähestymistapana. Se helpottaa päätöksentekijöitä tekemään riskinarviointia tehokkaammin. Tapahtumapuuanalyysi on analyysitekniikka, joka loogisesti kehittää visuaalisen mallin mahdollisista tuloksista, jotka käynnistävät tapahtuman. Menetelmä rajoittuu yhteen käynnistävään tapahtumaan ja ei ota huomioon järjestelmän riippuvuuksia. (Silvianita;Mohd.;& Kurian, 2011)

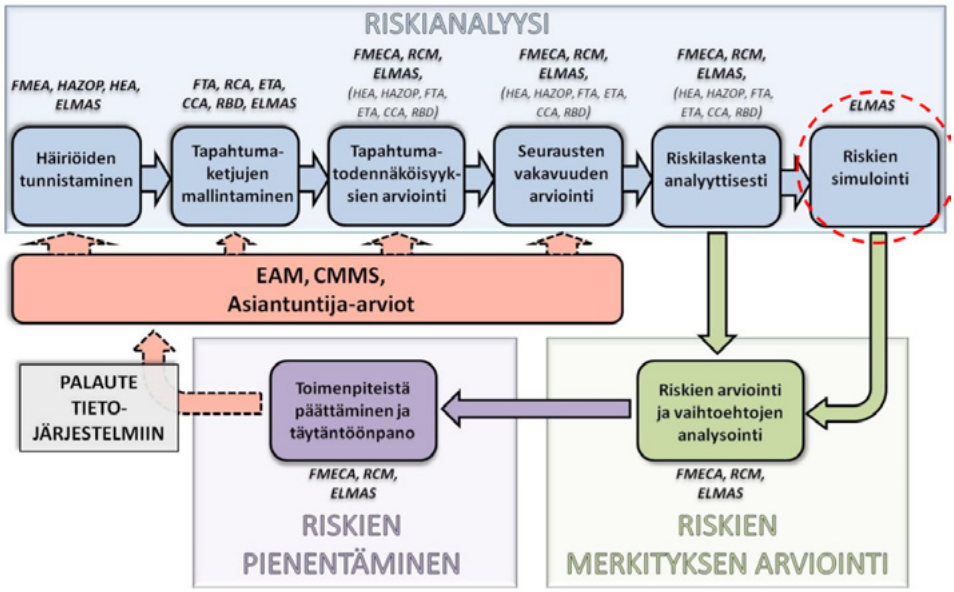


Kuva 24. Neljän riskianalyysin yhdistelmä (Silvianita;Mohd.;& Kurian, 2011)

Kuvassa 24 on esitetty integroitu riskinarviointimenetelmä alkaa FMEA-menettelyllä, joka liitetään vaaran tunnistamisksi HAZOP-menettelyyn. Prosessia jatketaan vika- ja tapahtumapuumenettelyillä. Vikapuun avulla tunnistetaan mahdolliset syyt ja tapahtumapuun avulla tunnistetaan kriittisten tapahtumien mahdolliset seuraukset. (Silvianita;Mohd.;& Kurian, 2011)

5.1.6 Yhdistetty FTA, CCA ja RBD

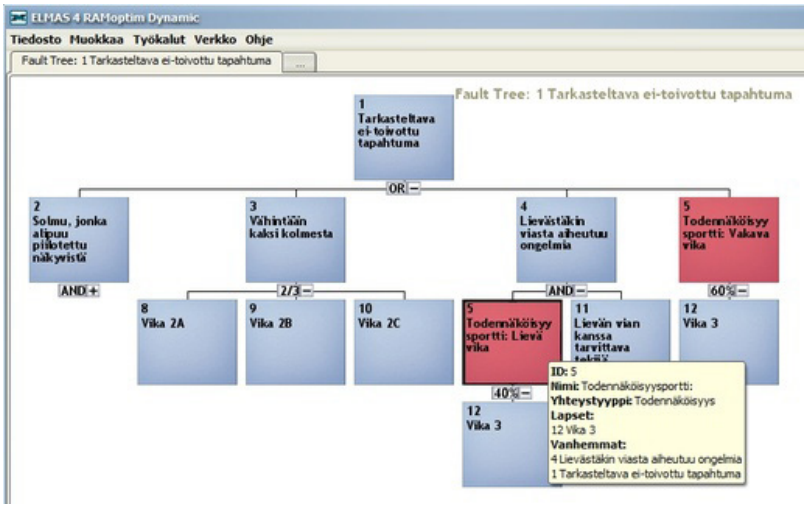
Ramentor Oy:n kehittämässä ELMAS (Event Logic Modeling and Analysis Software) ohjelmistossa voidaan mallintaa ja analysoida kohteen tapahtumien välistä loogista syy-seuraus-suhdetta. Muita tapahtumiin liittyviä ominaisuuksia, kuten esim. juurisyiden toteutumistaajuutta tai kustannuksia voidaan myös mallintaa. Kohteena voi olla esim. laite, järjestelmä tai prosessi sekä niiden vikaantuminen. (Ramentor Oy, 2016)
Alla olevassa kuvassa 25 on esitettynä, miten riskien hallintaa toteutetaan ELMAS ohjelmiston avulla.



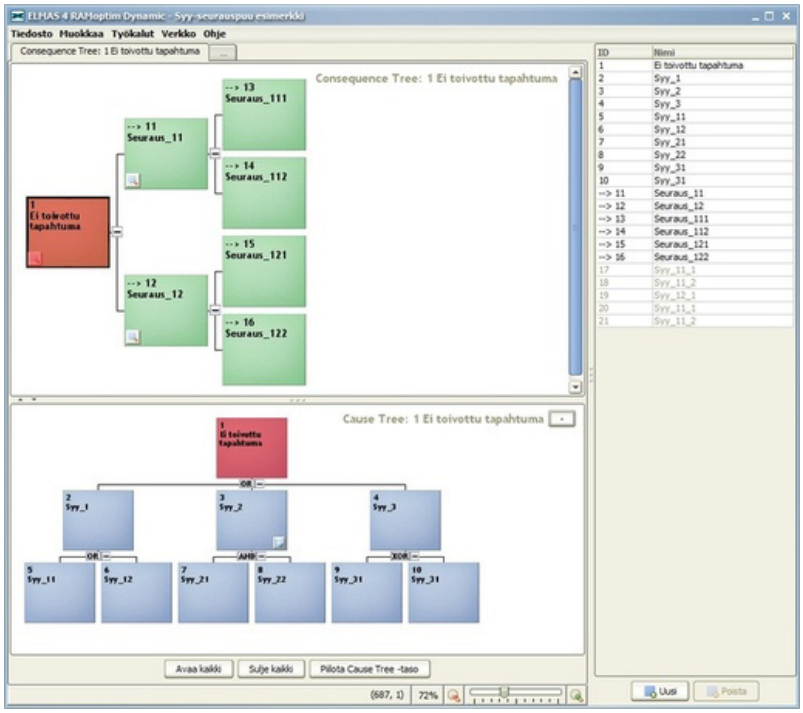
Kuva 25. Riskien hallintaa ELMAS ohjelmiston avulla (Lehtinen, 2012)

Ohjelmisto käyttää mm. kolmea erilaista mallinnustapaa, joita yhdistelemällä voidaan mallintaa monimutkaisiakin tapahtumaketjuja:

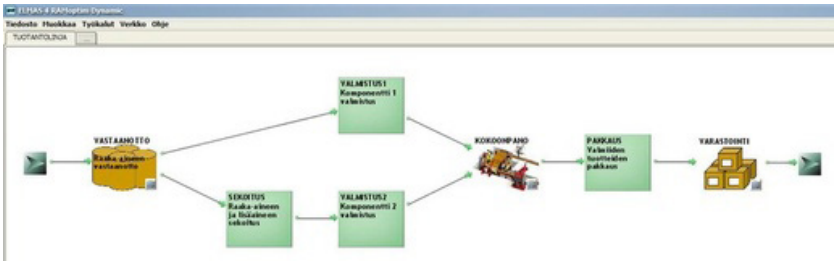
- Vikapuu - FTA (Fault Tree Analysis), kuva 26
- Syy-seurauspuu – CCA (Cause Consequence Analysis), kuva 27.
- Luotettavuuslohkokaavio – RBD (Reliability Block Diagram). (Ramentor Oy, 2016), kuva 28.



Kuva 26. Esimerkki ELMAS ohjelmistolla tehdystä vikapuumallista (Ramentor Oy, 2016)



Kuva 27. Esimerkki seurauspuumallista (Ramentor Oy, 2016)



Kuva 28. Esimerkki lohkokaaviomallista (Ramentor Oy, 2016)

5.1.7 Yhdistetty HAZOP- SIL - LOPA

Yleisesti hyväksyttävään riskitasoon pääsemiseksi erääseen työkaluun on yhdisttetty Hazop-, SIL- ja LOPA-menettelyt. Poikkeamatarkastelu HAZOP on prosessijärjestelmien riskien tarkempaan tunnistamiseen soveltuva menetelmä. HAZOPia täydennetään usein suojauskerrosanalyysillä (LOPA, Layers Of Protection Analysis sekä kokonaisturvallisuuden arvioinnilla (SIL, Safety Integrity Level). Nämä varmistavat riittävän suojaustason HAZOPissa tunnistettuja riskejä vastaan. LOPAn avulla lasketaan hyväksyttävä jäännösriski valituille tapahtumille, ottaen huomioon suojausten mahdollinen vioittuminen. Laskettua riskitasoa verrataan riskin sietotasoon sen määrittämiseksi, tarvitaanko lisäsuojausta. (AL Safety Design, 2015)

6 Yhteenveto

Teollisessa toiminnassa käytetään useita eri menetelmiä, jotta havaittaisiin ja pystyttäisiin ennakoimaan tuotanto-omaisuuden häiriö- ja ongelmatilanteita. Menetelmiä on kehitetty vuosia ja osa niistä on saavuttanut lähes standardimaisen aseman. Menetelmien kirjo aiheuttaa aika ajoin myös ongelmia johtuen mm. siitä, että niiden sisällöt ovat, tarkoituksesta huolimatta, samankaltaisia ja päällekkäisiä. Lisäksi niiden heikohko käytettävyys ovat olleet esteenä niiden joustavalle käytölle. Edellä mainittujen seikkojen vuoksi ja tueksi TPA-menetelmän kehityksessä haluttiin ottaa selville, millaisia päälekkäisiä menetelmiä on kehitetty ja mitä mahdollisia standardeja niissä on käytetty.

Tässä kirjallisuusselvityksessä tarkasteltiin myös muita mahdollisia menetelmiä ja erilaisia yhdistelmämenetelmiä, joiden nähtiin palvelevan TPA-menetelmän kehitystä. Selvityksen aikana vahvistui tieto erilaisten menetelmien suuresta kirjosta ja joidenkin huonosta käytettävyydestä ja laajuudesta. Huomattiin, että menetelmiä oli yhdistetty, mutta niiden käytettävyys oli jäänyt huomoimatta. Esimerkiksi ne ovat edelleen työläitä toteuttaa ja vaativat paljon resursseja. Myös riskin prioriteetin tunnistamiseen käytettiin edelleen samoja laskentatapoja, jotka voivat vääristää riskin vakavuuden luokittelua. Selvitys näyttäisi vahvistavan käsitystä siitä, että yhdistelmäriskianalyysimenetelmät ovat yleisemmin käytössä muualla maailmassa kuin Suomessa.

Tästä syystä saatiin vahvistusta kehittää edelleen TPA-menetelmää kaikille teollisuuden aloille sopivaksi analyysimenetelmäksi, jolla voidaan tunnistaa sekä turvallisuuden, ympäristön että talouden kannalta kriittisten poikkeamien esiintyminen niiden tuotantoprosesseissa. Tämä kirjallisuusselvitys toimii hyvänä pohjana geneerisen TPA-menetelmän luomisessa sekä vahvistaa yksinkertaisen TPA-menetelmän tarvetta. Selvityksessä on käytetty apuna mm. eri kirjallisuus-, Internet-, raportti- ja artikkelilähteitä.

Tämä julkaisu on tehty riskianalyysimenetelmien tarkastelu- ja kirjallisuusselvityksenä osana TPA-projektin työpakettia kaksi, jossa on selvitetty yleisimpien riskianalyysimenetelmien (VVKA, HAZOP, RCA ja riskianalyysi) käyttöä tulevassa TPA-menetelmässä. TPA-projektin tarkoituksena on tarkastella yleisimpien menetelmien parhaita puolia ja tarkastella epäkohtia sekä karsia päällekkäiset vaiheet uuden työkalun luomiseen. Tulevassa TPA-menetelmässä on tarkoituksena selvittää talouteen,

turvallisuuteen ja ympäristöön liittyvä kriittisyys siten, että käytetään minimimäärä menetelmiä ilman matemaattista tarkastelua. TPA-menetelmän pohjalta sovitaan toimenpiteet kriittisiksi todettujen tapahtumien ehkäisemiseksi tai vähintäänkin vahinkojen minimoimiseksi. Näitä toimenpiteitä voivat olla ennakoivat mittaukset, tarkistukset, huollot tai jopa muutokset kyseiseen prosessinosaan.

Lähdeluettelo

Aalipour, M.;Ayele, Y. Z.;& Barabadi, A. (2016). *Human reliability assessment (HRA) in maintenance of production process: A case study.* Haettu 12. 9 2016 osoitteesta http://munin.uit.no/bitstream/handle/10037/10382/article.pdf?sequence=5&isAllowed=y

AL Safety Design. (2015). *Yleisimpiä riskianalyysimenetelmiä.* Haettu 4. 4 2016 osoitteesta http://www.alsafety.com/riskianalyysi.html

Bell, J.;& Holroyd , J. (2009). *Review of human reliability assessment methods.* Derbyshire: Health and Safety Laboratory. Haettu 5. 10 2016 osoitteesta http://www.hse.gov.uk/research/rrpdf/rr679.pdf

Bowles, J. B. (2003). An assessment of RPN prioritization in a failure modes effects and criticality analysis. *Reliability and Maintainability Symposium, 2003. Annual* (ss. 380 - 386). IEEE. doi:10.1109/RAMS.2003.1182019

Bridges, W. (2008). *Selection of Hazard Evaluation Techniques.* Knoxville: Process Improvement Institute, Inc. (PII). Haettu 15. 7 2016 osoitteesta http://www.process-improvement-institute.com/_downloads/Selection_of_Hazard_Evaluation_Techniques.pdf

Casamirra, M.;Castaglia, F.;Giardina, M.;& Tomarchio, E. (2009). *Fuzzy modelling of HEART methodology: application in safety analyses of accidental exposure in irradiation plants.* Radiation Effects and Defects in Solids . doi:10.1080/10420150902805153

Clarke, P.;& Young, S. (Nov/Dec 2011). Reliability-centred maintenance and HAZOP - Is there a need for both? *maintenance & asset management vol 26 no 6,* 34 - 40. Haettu 7. 6 2016 osoitteesta Reliability -centered maintenance and HAZOP - Is there need for both?: http://www.maintenanceonline.co.uk/maintenanceonline/content_images/Pages%2034,35,36,37,38,39,40.pdf

Daramola, O.;Stålhane, T.;& Moser, T. (2011). A conceptual framework for semantic case-based safety analysis. *Emerging Technologies & Factory Automation (ETFA), 2011 IEEE 16th Conference on,* (ss. 1 - 8). doi:10.1109/ETFA.2011.6058981

Dittmann, L.;Rademacher, T.;& Zelewski, S. (2004). Performing FMEA Using Ontologies. *QR 2004 – 18th International Workshop on Qualitative Reasoning, 02.-04.08.2004 in.* Evanston (Illinois). Haettu 14. 6 2016 osoitteesta http://www.qrg.northwestern.edu/papers/files/qr-workshops/qr04/papers/DittmannRademacher-Zelewski-QR04.pdf

Frosdick, S. (1997). The techniques of risk analysis are insufficient in themselves. *Disaster Prevention and Management: An International Journal, Vol. 6 Iss: 3,* (ss. 165 - 177). Haettu 9. 6 2016

Giardina, M.;& Morale, M. (2015). *Safety study of an LNG regasification plant using an FMECA and HAZOP integrated methodology.* University of Palermo, Viale delle Scienze, Department of Energy, Information Engineering and Mathematical Models (DEIM),. 90128 Palermo, Italy: Journal of Loss Prevention in the Process Industries. doi:10.1016/j.jlp.2015.03.013

Guo, L.;& Kang, J. (11 2015). An extended HAZOP analysis approach with dynamic fault tree. *Journal of Loss Prevention in the Process Industries 38 (2015)* 224-232. doi:10.1016/j.jlp.2015.10.003

Heikkilä, A.-M.;Murtonen, M.;Nissilä, M.;Virolainen, K.;& Hämäläinen, P. (2007). *Riskianalyysien laatu: vaatimukset tilaajalle ja toteuttajalle.* Tampere: VTT. Haettu 5. 9 2016 osoitteesta http://www.vtt.fi/inf/julkaisut/muut/2007/Tutkimusraportti_VTT_R_03718_07.pdf

IEC. (2016). *About IEC publications - How does your numbering system work?* Haettu 12. 9 2016 osoitteesta https://webstore.iec.ch/webstore/webstore.nsf/xpFAQ.xsp?OpenXPage&id=GFOT-7NXLKU

Karjalainen, E. E. (5. 1 2016). *Riskiperusteinen ajattelu – Risk Based Thinking (RBT).* Haettu 23. 3 2016 osoitteesta http://www.sixsigma.fi/fi/artikkelit/rbt/

Khan, F.;Rathnayaka, S.;& Ahmed, S. (2015). Methods and models in process safety andrisk management: Past, present and future. *Process Safety and Environmental Protection volume 98 (2015)* (ss. 116-147). Elsevier B.V. doi:10.1016/S0957-5820(15)00202-5

Lee, J. C.;& McCormick, N. J. (Toim.). (2012). *Risk and Safety Analysis of Nuclear Systems.* John Wiley & Sons. Noudettu osoitteesta https://books.google.fi/books?id=mB5rLNJH534C&printsec=frontcover&dq=risk+and+safety+analysis+of+nuclear+systems+google+book&hl=fi&sa=X&ved=0ahUKEwjEterhkJjNAhVJIJoKHaQxA_gQ6AEIGTAA#v=onepage&q=inductive&f=false

Lehtinen, T. (24. 4 2012). Menetelmiä ja työkaluja käyttövarmuuden, riskien ja elinkaarikustannusten hallintaan. Noudettu osoitteesta http://www.psk-standardisointi.fi/Alasivut/Tiedotteet/Musiikkitalo_2012/1-Seminaarin%20avaus-Timo%20Lehtinen.pdf

Mollah, H.;Baseman, H.;& Long, M. (Toim.). (2013). *Risk Management Applications in Pharmaceutical and Biopharmaceutical Manufacturing* (4 p.). John Wiley & Sons. Haettu 8. 6 2016 osoitteesta https://books.google.fi/books?id=OASwudHANQYC&pg=PT29&hl=fi&source=gbs_toc_r&cad=3#v=onepage&q&f=false

Moubray, J. (1997). *Reliability-centered maintenance* (2. painos p.). New York: Industrial Press. Haettu 18. 12 2016 osoitteesta https://tpm4u.files.wordpress.com/2011/03/reliability-centered-maintenance-ii.pdf

Mäki, K. M. (18. 12 2016). RCM - Luotettavuuskeskeinen kunnossapito. Jyväskylä. Haettu 19. 12 2016

Nowlan, F. S.;& Heap, H. F. (1978). *Reliability-Centered Maintenance; report A066-579.* US Department of Commerce. Springfield, Virginia: National Technical Information Service. Haettu 18. 12 2016 osoitteesta https://web.archive.org/web/20130801183223/http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA066579

PSK 6800. (2008). Laitteiden kriittisyysluokittelu teollisuudessa. Noudettu osoitteesta http://www.psk-standardisointi.fi/index.htm

Ramentor Oy. (28. 7 2011). ELMAS 4; Vika-, vaikutus- ja kriittisyysanalyysi. Haettu 3. 2 2016 osoitteesta http://ramentor-com-bin.aldone.fi/@Bin/fff676dc0e3c418a8fad97cc5e14cb86/1469087855/application/pdf/1583477/ELMAS%204%20-%20FMEA.pdf

Ramentor Oy. (14. 6 2016). ELMAS - *Tapahtumalogiikan mallinnus ja analysointi.* Noudettu osoitteesta http://www.ramentor.com/etusivu/tuotteet/elmas/

Rantanen, E. (21. 10 2014). Riskienhallinta. Haettu 3. 6 2016 osoitteesta http://kuntatekniikka.fi/wp-content/themes/kuntatekniikka/images/pdf/skty/Eeva_Rantanen_Syyspaivat-14.pdf

Rauhala, V.;Kotkansalo, A.;Parkkila, L.;Siimes, A.;Sipola, J.;& Tarvainen, J. (2014). TP4: Criticality analysis on enviromental perspective and knowledge management in the prevention of sulphur emissions. Teoksessa S. Pitkäaho;& R. L. Keiski, *Sulphur Compounds in Mining Operations - Environmental Impact Assessment, Measurement and Emission Abatement* (ss. 50-67). Oulu, Suomi: Juvenes Print, Oulu. Haettu 13. 12 2016

Rong, M.;Zhao, T.;& Yu, Y. (2008). Advanced human factors Process Failure Modes and Effects analysis. *Reliability and Maintainability Symposium, 2008.* RAMS 2008. Annual (ss. 365 - 370). IEEE. doi:10.1109/RAMS.2008.4925823

Roth, M.;Wolf, M.;& Lindemann, U. (2015). Integrated Matrix-Based Fault Tree Generation and Evaluation. *Procedia Computer Science 44: 2015 Conference on Systems Engineering Research* (ss. 599-608). Elsevier B.V. Haettu 4. 7 2016

Sachdeva, A.;Kumar, P.;& Kumar, D. (2009). Maintenance criticality analysis using TOPSIS. 2009 *IEEE International Conference on Industrial Engineering and Engineering Management* (ss. 199 - 203). Hong Kong: IEEE. doi:10.1109/IEEM.2009.5373388

Sarsama, J.;Nissilä, M.;& Lehtinen, P. (2000). *Opas kattilalaitoksen vaaran arvioinnin laatimiseksi.* TUKES-julkaisu 4/2000, Helsinki. Haettu 13. 12 2016 osoitteesta http://docplayer.fi/3835597-Opas-kattilalaitoksen-vaaran-arvioinnin-laatimiseksi.html

SFS 5438. (1988). Järjestelmän luotettavuuden analysointimenetelmät. Vika- ja vaikutusanalyysi (VVA). Suomen standardisoimisliitto SFS.

SFS-EN 31010. (2013). Riskien hallinta. Riskien arviointimenetelmät. Suomen standardisoimisliitto SFS. Haettu 29. 1 2016

SFS-EN 60300-3-11:en. (5. 10 2015). Dependability management - Part 3-11: Application guide - Reliability centred maintenance. Suomen standardoimisliitto SFS. Haettu 7. 7 2016

SFS-EN 60812:en. (11. 9 2006). Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA). Helsinki: Suomen standardoimisliitto SFS ry. Haettu 9. 5 2016

SFS-EN 61025:en. (17. 12 2007). Fault tree analysis (FTA). Helsinki: Suomen Standardisoimisliitto SFS ry. Haettu 5. 10 2016

SFS-EN 61882:en. (17. 6 2016). Hazard and operability studies (HAZOP studies). Application guide. Haettu 5. 10 2016

SFS-EN 62508:en. (24. 1 2011). Guidance on human aspects of dependability. Helsinki: Suomen standardoimisliitto SFS ry. Haettu 5. 10 2016

SFS-EN 62740:en. (10. 8 2015). Root Cause Analysis (RCA). Suomen standardisoimisliitto SFS. Haettu 5. 10 2016

SFS-IEC 60300-3-9. (30. 6 2000). Luotettavuusjohtaminen osa 3: käyttöopas. Luku 9: teknisten järjestelmien riskianalyysi. Suomen standardisoimisliitto SFS. Haettu 3. 12 2015

SFS-ISO 31000. (5. 10 2011). Riskienhallinta. Periaatteet ja ohjeet. Suomen standardoimisliitto SFS.

Silvianita, S.;Mohd., F. K.;& Kurian, V. J. (2011). Critical Review of a Risk Assessment Method and its Applications. *2011 International Conference on Financial Management and Economics, IPEDR vol.11* (2011). Noudettu osoitteesta http://www.ipedr.com/vol11/16-R10014.pdf

Suutama, M. (2015). *Hiertämön laitteiden käyttövarmuuden ja kunnossapidon arviointi ja kehittäminen.* Teknillisten tieteiden tiedekunta. Tampere: Tampereen teknillinen yliopisto. Haettu 11. 5 2016 osoitteesta http://dspace.cc.tut.fi/dpub/bitstream/handle/123456789/23594/suutama.pdf?sequence=1

Terveyden ja hyvinvoinnin laitos. (30. 6 2015). *Vaaratapahtuman tunnistaminen.* Haettu 21. 1 2016 osoitteesta https://www.thl.fi/fi/web/laatu-ja-potilasturvallisuus/tutkimus-ja-kehittaminen/tyokalut/vaaratapahtuman-tunnistaminen

Trammell, S. R.;& Davis, B. J. (2001). Using a Modified Hazop/FMEA Methodology for Assessing System Risk. *Engineering Management for Applied Technology, 2001. EMAT 2001. Proceedings. 2nd International Workshop on* (ss. 47 - 53). Austin, TX: IEEE. doi:10.1109/EMAT.2001.991310

Trammell, S. R.;Lorenzo, D. K.;& Davis, B. J. (4 2004). Integrated Hazards Analysis: Using the Strengths of Multiple Methods to Maximize Effectiveness. *Professional Safety,* 29-37. Haettu 31. 5 2016 osoitteesta http://aeasseincludes.asse.org/professionalsafety/pastissues/049/05/020504as.pdf

Työturvallisuuskeskus. (2003). Työturvallisuuslaki (738/2002). (9). Helsinki: Työturvallisuuskeskus. Haettu 6. 9 2016 osoitteesta http://ttk.fi/files/1196/Tyoturvalaki_suomi.pdf

Työturvallisuuskeskus. (1. 6 2015). Riskien arviointi työpaikalla -työkirja. Haettu 13. 6 2016 osoitteesta http://ttk.fi/files/2941/Riskien_arviointi_tyopaikalla_tyokirja_22052015_kerttuli.pdf

Työturvallisuuskeskus. (2016_a). *Työturvallisuus- ja työterveysriskien tunnistaminen ja arviointi*. Haettu 6. 9 2016 osoitteesta Lomakkeet riskien arvioinnin suunnitteluun: http://ttk.fi/tyohyvinvointi_ja_tyosuojelu/toiminta_tyopaikalla/vastuut_ja_velvoitteet/tyon_vaarojen_selvittaminen_ja_arviointi

Työturvallisuuskeskus. (2016_b). Riskianalyysin yhteenvetolomake. Noudettu osoitteesta http://ttk.fi/files/3283/Riskianalyysin_yhteenvetolomake.pdf

US_EPA. (07-08 2008). Process Hazard Analysis (PHA). *Chemical emergency preventetion & planning, Newsletter.* Seattle, Washington, USA. Haettu 11. 7 2016 osoitteesta https://www3.epa.gov/region10/pdf/rmp/cepp_newsletter_0708.pdf

Weibull. (2015). *Failure Mode and Effect Analysis (FMEA) and Failure Modes, Effects and Criticality Analysis (FMECA).* Haettu 9. 3 2016 osoitteesta http://www.weibull.com/basics/fmea_fig1.htm

Vesely, W. E.;Goldberg, F. F.;Roberts, N. H.;& Haasl, D. F. (1981). *Fault Tree Handbook.* Washington, D.C. 20555: U.S. Nuclear Regulatory Commission . Haettu 8. 6 2016 osoitteesta http://www.nrc.gov/docs/ML1007/ML100780465.pdf

Wessberg, N.;Seppälä, J.;Molarius, R.;Koskela, S.;Pennanen, J.;Silvo, K.;& Kekoni, P. (2006). *Häiriöpäästöjen ympäristöriskianalyysi.* Suomen ympäristökeskus. Haettu 5. 4 2016 osoitteesta http://www.tukes.fi/Tiedostot/vaaralliset_aineet/esitteet_ja_oppaat/Hairiopaastojen_ympriskianalyysi.pdf

Wilbur, D. (18. 11 2016). *Human Factors: Challenging Traditional Assumptions and Methods That Focus on the Actions of individuals.* Haettu 2016 osoitteesta Arms reliability, Featured blog: http://blog.armsreliability.com/blog

Liiteluettelo

Standardi	Englanninkielinen nimi	Työkalut ja tekniikat	Kuvaus ja käyttö	Riskiarviointiprosessi				
				Riskin tunnistaminen	Riskianalyysi			Riskin merkityksen arviointi
					Seuraus	Todennäköisyys	Riskitaso	
SFS-EN ISO 14001 Ympäristöjärjestelmät. Vaatimukset ja niiden soveltamisohjeita: 2015	Environmental risk assessment Toxicological risk assessment	Ympäristöriskien arviointi Myrkyllisten aineiden riskinarviointi	Vaarat tunnistetaan ja analysoidaan ja mahdolliset tavat, joilla määritelty kohde voi joutua vaaraan, tunnistetaan. Tiedot altistumisen tasosta ja haittojen luonteesta johtuen tietyn tasoisesta altistumisesta, yhdistetään antamaan todennäköisyysarvo sille, että määritetty vahinko tapahtuu.	++	++	++	++	++
SFS-EN 60300-3-11:en Dependability management - Part 3-11: Application guide - Reliability centred maintenance (RCM): 2015	Reliability centred maintenance (RCM)	Toimintavarmuus- keskeinen kunnossapito	Menetelmä menettelytapojen tunnistamiseen, jotka olisi toteutettava vikojen hallitsemiseen niin, että tehokkaasti saavutetaan kaikentyyppisten laitteiden vaadittu turvallisuus, käyttövarmuus ja taloudellisuus. Kaikki tehtävät perustuvat henkilöstön ja ympäristön osalta turvallisuuteen ja ne koskevat myös käyttöä ja taloudellisuutta. Suurin hyöty saavutetaan kohdistamalla analyysi sinne, missä vikaantumisella olisi vakavia turvallisuuteen, ympäristöön, talouteen tai käyttötoimintaan liittyviä vaikutuksia.	++	++	++	++	++
SFS-EN 60812:en Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA):2006	Failure modes and effects analysis (FMEA) and failure modes and effects and criticality analysis (FMECA)	Vika- ja vaikutusanalyysi (FMEA), vikatyyppien ja vaikutusten ja kriittisyyden arviointi (FMECA)	FMEA on tekniikka, joka tunnistaa vikamuodot ja -mekanismit ja niiden vaikutukset. FMEA:ta voi seurata kriittisyysanalyysi, jossa määritellään kunkin vikamuodon merkitys laadullisesti, puolilaadullisesti tai määrällisesti (FMECA). Kriittisyysanalyysi voi perustua todennäköisyyteen, että vikamuoto johtaa järjestelmän vikaan, tai riskitasoon siihen liittyvän vikamuodon kanssa, tai riskin prioriteettinumeroon. Vaarojen tunnistamisen ja taajuuden analysoinnin perusmenetelmä.	++	++	++	++	++

Menetelmä, joka toteutettavissa esim. excel ohjelmalla	Structure « What if? » (SWIFT)	Rakenne « Mitä jos? » (SWIFT) Järjestelmä, jossa ryhmää kehotetaan tunnistamaan riskejä (helpottaa työtä työrymissä). On sidoksissa riskianalyysiin ja riskin arviointitekniikkaan. ++ ++				++	++	++
SFS-EN 62508:en Guidance on human aspects of dependability: 2011	Human reliability assessment (HRA)	Ihmisen luotettavuuden analyysi	Taajuusanalyysitekniikka, joka tarkastelee ihmisen vaikutusta järjestelmän toimintaan ja arvioi ihmisen virheiden vaikutusta luotettavuuteen	++	++	++	++	+
riskitaso luetaan riskimatriisista	Consequence/ probability matrix	Seuraus/ todennäköisyys matriisi	Seuraus-todennäköisyysmatriisi on keino yhdistää seurauksen ja todennäköisyyden laadullinen tai puolimäärällinen luokitus riskitason tai riskiluokituksen tuottamiseksi. Seuraus-todennäköisyys-matriisia käytetään riskien luokitukseen, riskin lähteisiin tai riskin käsittelyyn riskitason perusteella. Sitä käytetään yleisesti seulontatyökaluna, kun on tunnistettu useita riskejä, esimerkiksi määrittelemään mitkä riskit tarvitsevat lisä- tai yksityiskohtaisempaa analyysiä, mitkä riskit täytyy käsitellä ensin tai mitkä täytyy siirtää korkeamman johtotason hallintaan (tai jotka eivät sillä kertaa tarvitse jatkotarkastelua).	++	++	++	++	+
SFS-EN 62740:en Root cause analysis (RCA): 2015	Root cause analysis (RCA)	Juurisyiden analyysi	Yksittäinen vahinko, joka on tapahtunut, analysoidaan tarkoituksena ymmärtää siihen myötävaikuttaneet syyt ja miten järjestelmää tai prosessia voi parantaa välttämällä tulevaisuudessa samoja vahinkoja. Analyysissä on tarkasteltava mitkä valvontamenettelyt olivat jo käytössä, kun vahinko tapahtui, ja kuinka valvontamenettelyä voisi parantaa.	-	++	++	++	++
SFS-EN 62740:en Root cause analysis (RCA): 2015	Root cause analysis (RCA)	Juurisyiden analyysi	Yksittäinen vahinko, joka on tapahtunut, analysoidaan tarkoituksena ymmärtää siihen myötävaikuttaneet syyt ja miten järjestelmää tai prosessia voi parantaa välttämällä tulevaisuudessa samoja vahinkoja. Analyysissä on tarkasteltava mitkä valvontamenettelyt olivat jo käytössä, kun vahinko tapahtui, ja kuinka valvontamenettelyä voisi parantaa.	-	++	++	++	++

Menetelmä, joka toteutettavissa esim. excel ohjelmalla	Scenario analysis	Skenaario-analyysi	Mahdolliset tulevaisuuden skenaariot tunnistetaan mielikuvitusta käyttämällä tai ekstrapoloimalla nykyisistä ja erilaisista riskeistä ottaen huomioon, että jokainen näistä skenaarioista saattaa esiintyä. Tämä voidaan tehdä muodollisesti tai epämuodollisesti, määrällisesti tai laadullisesti.	++	++	+	+	+
	Risk indices	Riski-indeksit	Riski-indeksi on puolimäärällinen riskin mitta, joka saadaan arviona käyttämällä pisteytysmenettelytapaa käyttävää järjestysasteikkoa. Riski-indeksiä voidaan käyttää monien riskien arviointiin käyttäen samanlaista kriteeriä siten, että niitä voidaan verrata. Pistemääriä sovelletaan riskin jokaiseen komponenttiin. Riski-indeksit ovat olennaisilta osiltaan laadullinen menettelytapa luokittelemaan ja vertailemaan riskejä. Numeroiden käyttö yksinkertaistaa käsittelyä.	+	++	++	+	++
Vikapuuanalyysin SFS-EN 61025:en Fault tree analysis (FTA): 2007 ja tapahtumapuuanalyysin yhdistelmä/ kaaviollinen esitys	Cause and consequence analysis	Syy- ja seuraus-analyysi	Vika- ja tapahtumapuun yhdistelmä, johon voidaan sisällyttää aikaviiveet. Alkutapahtuman sekä syitä että seurauksia tarkastellaan. Alkutapahtumana pidetään sekä syitä että seurauksia. Vaarojen tunnistamis- ja taajuusanalyysitekniikka, joka alkaa ei toivotusta tapahtumasta ja määrittää kaikki siihen johtavat tapahtumaketjut. Nämä esitetään graafisesti.	+	++	++	+	+
	Decision tree	Päätöspuu	Päätöspuu edustaa päätösvaihtoehtoja ja tuloksia peräkkäin tavalla, joka ottaa huomioon myös epävarmat tulokset. Se alkaa alkutapahtumasta tai alkupäätöksestä ja mallintaa erilaisia reittejä ja tuloksia mahdollisten tapahtumien sekä erilaisten tehtyjen päätösten tuloksina. Päätöspuuta käytetään projektiriskienhallinnassa ja muissa tapauksissa auttamaan parhaan toimintatavan valitsemisessa epävarmoissa tilanteissa. Graafinen esitys voi myös helpottaa viestimään päätöksien perustelut.	-	++	++	+	+

FN curves (frequency (F) at which N or more)	FN käyrät (uhri-luvut)	FN-käyrät ovat graafisia esityksiä sellaisten tapahtumien todennäköisyyksistä, jotka aiheuttavat tietyn tasoisista vahinkoa tietylle väestöryhmälle (viittaavat tietyn uhrilukumäärän esiintymistaajuuteen). Ovat yksi tapa esittää riskianalyysin tuotoksia. Monilla tapahtumilla on suuri todennäköisyys ja vähäiset seuraukset sekä pieni todennäköisyys ja suuret seuraukset. FN-käyrät esittävät riskin tason viivana. FN-käyriä voidaan käyttää joko järjestelmien tai prosessien suunnittelussa tai olemassa olevan järjestelmän hallinnassa.	+	++	++	+	++
Multi-criteria decision analysis (MCDA)	Monikriteeri-analyysi (MCDA)	Tavoitteena on käyttää erilaisia kriteereitä objektiivisesti ja läpinäkyvästi arvioitaessa vaihtoehtojoukon yleistä varteenotettavuutta. Yleisesti kaiken kaikkiaan tavoitteena on tuottaa suosituksia saatavilla olevien vaihtoehtojen välillä. Analyysiin sisältyy vaihtoehtojen matriisin kehittäminen ja kriteerit, jotka on luokiteltu ja ryhmitelty siten, että saadaan jokaiselle vaihtoehdolle kokonaispisteytys.	+	++	+	++	+
Bow tie analysis	Rusettianalyysi	Yksinkertainen kaavamainen tapa kuvata ja analysoida riskin polut vaaroista tuloksiin ja tarkistaa hallintakeinoja. Sitä voidaan pitää yhdistelmänä tapahtuman syyn loogisesta vikapuunanalysoinnista (edustaa solmu-kohtaa) ja seurausten tapahtumapuuanaly-soinnista.	-	+	++	++	+
Business impact analysis (BIA)	Liiketoi-minta-analyysi	Analysoidaan, miten keskeiset keskeyty-misriskit voivat vaikuttaa organisaation toimintaan sekä tunnistaa ja määrittää voimavarat, jotka vaadittaisiin asian hallit-semiseksi.	+	++	+	+	+

	Cost/benefit analysis (CBA)	Kustannus/hyöty analyysi	Kustannus-hyötyanalyysiä voidaan käyttää riskin arviointiin missä odotettuja kokonaiskuluja punnitaan vasten odotettuja kokonaishyötyjä tarkoituksena valita paras tai kannattavin vaihtoehto. Se on monen riskinarviointijärjestelmän olennainen osa. Se voi olla laadullinen tai määrällinen tai voi sisältää määrällisten ja laadullisten elementtien yhdistelmän. Määrällinen kustannus-hyötyanalyysi yhdistää kaikkien kustannusten rahallisen arvon ja kaikki hyödyt kaikille osapuolille (mukautuu erilaisille ajanjaksoille, joiden aikana kustannukset ja hyödyt kertyvät).	+	++	+	+	+
SFS-EN 62502:en Analysis techniques for dependability - Event tree analysis (ETA): 2011	Event tree analysis (ETA)	Tapahtumapuu-analyysi	Tekniikka, joka alkaa ei-toivotulla tapahtumalla (päätapahtuma) ja määrittää kaikki ne tavat, joilla se voisi tapahtua. Ne näytetään graafisesti loogisessa puukaaviossa. Kun vikapuu on kehitetty, olisi pohdittava keinoja, joilla voitaisiin vähentää tai poistaa mahdolliset syyt/lähteet.	+	++	+	+	-
IEC 61508 (all parts), Functional safety of electrical/electronic/programmable electronic safety-related systems IEC 61511, Functional safety – Safety instrumented systems for the process industry sector	Layer protection analysis (LOPA)	Kerrossuojaus-analyysi (LOPA)	LOPA-analyysi on puolimäärällinen menetelmä, jolla arvioidaan epätoivottuun tapahtumaan tai ennusteeseen liittyvät riskit. (Voidaan kutsua myös esteiden analyysiksi). Valitaan syy-seurauspari ja tunnistetaan suojauskerrokset, jotka torjuvat syyn aiheuttamasta epätoivottua seurausta. Lasketaan suuruusluokka sen määrittämiseksi, onko suojaus riittävä pienentämään riskin siedettävälle tasolle. LOPA-analyysiä voidaan käyttää laadullisesti tarkistamaan yksinkertaisesti suojauskerrokset vaara- tai syytapahtuman ja lopputuloksen välillä.	+	++	+	+	-

Kirjoittajat

Tarvittaessa yhteydenotot: etunimi.sukunimi@lapinamk.fi

Kotkansalo, Arja
Insinööri (ylemipi AMK)
projektipäällikkö TPA-hankkeessa
Käynnissäpidon tutkimus, Operation and Maintenance Research (O&M)
Teollisuuden ja luonnonvarojen osaamisala, Lapin ammattikorkeakoulu

Parkkila, Leena
Insinööri (ylempi AMK)
projekti-insinööri
Käynnissäpidon tutkimus, Operation and Maintenance Research (O&M),
Teollisuuden ja luonnonvarojen osaamisala, Lapin ammattikorkeakoulu

Tarvainen, Jaana
Insinööri (ylempi AMK)
projekti-insinööri TPA hankkeessa 1.10.2015-30.3.2017 välisenä aikana
Käynnissäpidon tutkimus, Operation and Maintenance Research (O&M)
Teollisuuden ja luonnonvarojen osaamisala, Lapin ammattikorkeakoulu

Teollisessa toiminnassa käytetään useita eri menetelmiä, jotta havaittaisiin ja pystyttäisiin ennakoimaan tuotanto-omaisuuden häiriö- ja ongelmatilanteita. Menetelmiä on kehitetty vuosia ja osa niistä on saavuttanut lähes standardimaisen aseman. Menetelmien kirjo aiheuttaa aika ajoin myös ongelmia johtuen mm. siitä, että niiden sisällöt ovat, tarkoituksesta huolimatta, samankaltaisia ja päällekkäisiä. Myös näiden menetelmien heikohko käytettävyys ovat olleet esteenä niiden joustavalle käytölle. Tässä julkaisussa on selvitetty yleisempien menetelmien (VVKA, HAZOP, RCA ja riskianalyysi) parhaat puolet, tarkasteltu niiden epäkohtia sekä karsittu päällekkäisiä vaiheita uuden työkalun tapauskohtaista luomista varten.

Tämä julkaisu on tehty riskianalyysimenetelmien tarkastelu- ja kirjallisuusselvityksenä, joka toimii pohjana hankkeessa kehitettävälle Tuotannon poikkeama analyysi (TPA) -menetelmälle. Kehitettävän menetelmän lähtökohtana ja tavoitteena on kehittää TPA kaikille teollisuuden aloille sopivaksi analyysimenetelmäksi, jolla voidaan tunnistaa sekä turvallisuuden, ympäristön että talouden kannalta kriittisten poikkeamien esiintyminen niiden tuotantoprosesseissa.

Julkaisu liittyy Lapin ammattikorkeakoulun käynnissäpitotutkimusryhmän toteuttamaan TPA – Tuotannon poikkeama analyysi – hankkeeseen, joka toteutetaan 1.10.2015 – 30.9.2018 välisenä aikana. Hanketta rahoittaa Lapin liiton ja Lapin ammattikorkeakoulun lisäksi mukana olevat yrityspartnerit, joita ovat Agnico Eagle Finland Oy, Kemin Kaupunki tilapalvelu, SMA Mineral Oy ja Etteplan Design Center Oy Kemin toimisto.

O&M Operation and Maintenance research

LAPIN LIITTO

Vipuvoimaa EU:lta 2014–2020

Euroopan unioni
Euroopan aluekehitysrahasto

LAPIN AMK
Lapland University of Applied Sciences

www.lapinamk.fi

ISBN 978-952-316-200-6